VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA PRÁVA

Počítačová kriminalita a sociální hacking

Computer Crime and Social Hacking

Študent: Martin Tupý

Vedúci diplomovej práce: JUDr. Bohuslav Halfar

Ostrava 2014

Prohlášení

Prohlašuji, že jsem bakalárskou práci vypracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých sem čerpal.

V Ostravě dne 7.5.2014

.....

podpis

Obsah

1 ÚVOD

Druhá polovica 20. storočia priniesla ľudstvu výrazný rozvoj informačných technológií. V dnešnej dobe je bežné, že sa s informačnými technológiami stretávame na každom kroku, či už v oblasti výroby, obchodu, komunikácie alebo zábavy. Taktiež sme svedkami toho, ako sa postupne preberajú a automatizujú niektoré časti ľudských činností. Ľuďom však snaha maximalizovať svoje zisky zatienila myseľ a tak, aj keď nelegálnou cestou, chcú využiť technológie vo svoj prospech. Preto táto nová éra počítačov so sebou prináša aj jedno veľké riziko, a to bezpečnostné.

Nič nebránilo tomu, aby mohol vzniknúť ďalší fenomén tejto doby, známy ako počítačová kriminalita. Vzhľadom na neuveriteľný rozvoj bolo už len otázkou času, kedy sa niečo podobné objaví. Tento druh kriminality má jednu obrovskú výhodu a to tú, že páchateľ už nemusí byť fyzicky na mieste činu, ale delikt môže páchať z pohodlia domova resp. z miesta, ktoré si sám zvolí ako bezpečné a pohodlné. Pri fakte, že internet a s ním spojené sociálne siete určené na komunikáciu využíva 80% mladých Európanov[1], môžeme hovoriť o výraznom náraste, pokroku a rozvoji komunikácie za posledné dve až tri dekády. Taktiež sú rozšírené aj rôzne platobné transakcie, ktorých objem činil v roku 2011 približne 8 biliónov USD[2]. Práve toto je jeden z faktorov, prečo sa stále viac rozširuje kriminalita páchaná prostredníctvom počítača a zariadení spojených s výpočtovou technikou.

Každým dňom sa stáva obeťou počítačovej kriminality približne milión ľudí po celom svete. Trestná činnosť vo virtuálnom prostredí zahŕňa rôzne delikty. Či už ukradnutie údajov od platobných kariet, kradnutie totožnosti, sexuálne zneužívanie až po závažné kybernetické útoky na rôzne tuzemské a medzinárodné inštitúcie. Rozsah počítačovej kriminality sa snaží popísať mnoho dokumentov, najvhodnejším a najpresnejším sa z môjho pohľadu zdá byť preambula manuálu pre prevenciu a kontrolu počítačového zločinu OSN, ktorý sa spomína v tejto práci.

Pri pokuse skúmania problematiky moderných informačných technológii je treba mať neustále na pamäti základný problém. Rozvoj v tejto oblasti je natoľko dynamický, že pokus

[1] EUROSTAT. Internet access and use in 2010. In: [online]. [cit. 2014-05-04]. Dostupné z: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-14122010-BP/EN/4-14122010-BP-EN.PDF

[2] PÉLISSIÉ DU RAUSAS, M.- MANYIKA J.- HAZAN E. et al. 2011. *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity.* [online]. 2011. [cit. 2014-05-04]. Dostupné z: http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

o teoretické alebo vedecké skúmanie sa stane automaticky zastaraným už v momente prvého uverejnenia, tzv. permanentná revolúcia[3].

Pre prácu sú definované nasledovné hypotézy. Počítačová kriminalita spolu so sociálnym hackingom sú najbežnejším javom, ktorý napĺňa skutkovú podstatu trestného činu alebo inak protiprávneho jednania v poslednej dekáde. Monitorovanie ľudí štátnymi a súkromnými zložkami neslúži iba na bezpečnosť a ochranu. Internet prestáva byť miesto, kde je človek anonymný a zároveň začína byť veľmi ľahko napadnuteľný. Sociálne siete sa stali prostriedkom na obchodovanie a zneužívanie osobných dát. Cieľom práce je poukázať na nebezpečenstvo internetu z hľadiska užívateľa, jeho zneužívanie, poukázanie na monitorovanie používateľov z rôznych strán a taktiež aj právne vymedzenie pojmu počítačová kriminalita.

K potvrdeniu alebo falzifikácii hypotéz a zároveň k dosiahnutiu cieľa budem využívať metódu analýzy a syntézy a metódu indukcie .

O samotnej počítačovej kriminalite a jej problematike je v dnešnej dobe obrovské množstvo informácii, avšak iba malá časť týchto materiálov má klasickú, a teda tlačenú formu. Základným zdrojom sa teda stáva samotný internet. Má to však určitý problém a to je overenie a relevantnosť informácii. V prostredí virtuálnej reality je to veľmi náročné, niekedy až nemožné a preto je potreba pristupovať k získaným dátam s rozvahou.

[3] MATĚJKA, Michal. *Počítačová kriminalita*. 2002. vyd. Praha: Comupter Press, 2002, s. 4

2 História počítačovej kriminality

Počítačová kriminalita je pojem, ktorý sa začína objavovať v médiách čím ďalej, tým častejšie. Mnohí si myslia, že počítačová kriminalita je jav, ktorého počiatky nesiahajú ďalej, ako do posledných dvoch – troch desaťročí. Nie je to však pravda. Tento pojem je omnoho starší, ako si široká verejnosť môže myslieť a jeho úplné počiatky sa datujú niekde do začiatku 19. storočia.

2.1 Úvod do histórie počítačovej kriminality

Pojem počítačová kriminalita označuje trestné činy páchané pomocou počítača resp. na počítači. Počítačová kriminalita ide ruka v ruke s technologickým postupom a inováciou. Preto čím dokonalejšie technológie sú dostupné pre užívateľov, tým sú rovnako dostupné aj pre ľudí ktorí majú záujem o zneužívanie technológii. *Hackeri*[4] a teda počítačoví špecialisti alebo programátori s detailnými znalosťami fungovania systému; dokážu s ním výborne pracovať a najmä si ho upraviť podľa svojich potrieb alebo *crackeri*[5] - osoby prenikajúce do cudzích počítačov či databáz (cez sieť) bez toho, aby mali prístupové práva. Základný rozdiel medzi hackerom a crackerom spočíva v tom, že hacker veci vytvára a cracker ich neoprávnene napáda a mení vo svoj prospech, prípadne v prospech niekoho napr. keď koná na objednávku.

Pre ďalšie pokračovanie je nutné aby som uviedol historické členenie. Najvhodnejšie je členenie podľa publikácie Michala Matějky[6] a teda:

- obdobie od vynálezu telefónu po uvedenie prvého PC na trh označujeme ako *pravek,*
- obdobie od roku 1981 do prípadu Citibank v roku 1994 (stredovek),
- obdobie od roku 1994 do dnes sa nazýva novovekom počítačovej kriminality.

2.2 Pravek

V období do roku 1981 sa nedá hovoriť o masovom rozširovaní počítačovej kriminality, pretože počet počítačov v tej dobe bol zanedbateľný rovnako ako ich využitie. Prvé počítače boli príliš drahé, veľmi veľké, taktiež boli strážené a malo k ním prístup iba niekoľko „vyvolených“ programátorov. V tej dobe vzniklo aj slovo hacker. Ako bolo v úvode spomenuté, za hackera sa považuje človek, ktorý si programy upravuje podľa vlastnej potreby. Tak, aby fungovali lepšie, rýchlejšie, efektívnejšie a teda, aby boli pre neho, prípadne pre prácu niekoho iného, celkovo

[4] Matějka, M.: *Počítačová kriminalita*. Praha: Vydavatelství a nakladatelství Computer Press, 2002. s. 20
[5] Matějka, M.: *Počítačová kriminalita*. Praha: Vydavatelství a nakladatelství Computer Press, 2002. s. 12
[6] Matějka, M.: *Počítačová kriminalita*. Praha: Vydavatelství a nakladatelství Computer Press, 2002. s. 17

prijateľnejšie. Takýmto zásahom sa hovorilo *hacks*. Tieto termíny však postupom času začali získavať aj iný zmysel a dnes si tento pojdem ľudia spájajú skôr s útokom pomocou počítača.

Za úplne prvý zločin sa však považuje prípad, ktorý sa stal v roku 1801 vo Francúzsku. Istý pán Jacquard zostrojil primitívne zariadenie, ktoré dovoľovalo automaticky pomocou dierkových štítkov opakovane vykonávať určité úkony, ktoré bolo treba pri tkaní špeciálnych druhov látok. Zamestnanci pána Jacquarda však zo strachu pred stratou zamestnania vynález neprijali a snažili sa ho sabotovať. Nakoniec dosiahli to, že pán Jacquard už nepokračoval na v ďalšom vývoji a zdokonaľovaní stroja.

Posun nastal 14. Februára v roku 1946, kedy bol zostrojený prvý elektrónkový počítač známy pod menom ENIAC *(Electronic Numerical Integrator And Computer)*[7]. Tento dátum je v análoch zapísaný ako deň kedy sa zrodil počítačový vek. Samozrejme ENIAC bol iný počítač, ako počítače, ktoré sú v súčasnosti. Mal asi 30 ton (spolu s chladením), zaberal 63m^3 a „konzumoval“ asi 200 kilowattov. Samozrejme takýto počítač nemohol a nemal ako slúžiť na počítačovú kriminalitu. Či už kvôli nákladom na obstaranie, alebo pre veľkosť a energetickú náročnosť.

V tom období sa a napriek tomu udialo niekoľko kriminálnych deliktov. Známy je prípad *Cap ´n ´Crunch*, ktorý dostal pomenovanie podľa značky cereálií. Do týchto cereálií výrobca pridával detskú píšťalku, ktorá vydávala zvuk o frekvencií 2600 Hz. Túto frekvenciu používala telefónna spoločnosť AT&T k vnútornej signalizácií v sieti. Používateľ píšťalky spolu so zariadením Blue box dosiahol to, že volajúci volal zadarmo. Ako prvý si to všimol John Draper[8] . Zverejnením tohto a mnohých ďalších poznatkov sa rozšírili nelegálne telefonáty. Tento druh kriminálnych skutkov dostal názov *phreaking*. Znamená to napojenie sa na cudziu telefónnu linku v rozvodniach, verejných telefónnych búdkach alebo priamo na nadzemné prípadne podzemné telefónne vedenie. Týmto termínom sa neskôr označovalo aj neoprávnené pripojenie na internet, prípadne odpočúvanie iných telefonických rozhovorov.

V Českej republike je známy prípad zo 70. rokov. Bol to jeden z prvých prípadov zaoberajúci sa počítačovou kriminalitou. Nespokojný pracovník Úradu dôchodkového zabezpečenia poškodzoval magnetom záznamy na magnetických páskach. Pracovník dostal viac ako 10 ročný trest za sabotáž.

[7] WEIK, M. *The Eniac Story* [online]. 1961 [cit. 2014-05-05]. Dostupné z: http://ftp.arl.mil/mike/comphist/eniac-story.html
[8] Matějka, M. *Počítačová kriminalita*. Praha: Vydavatelství a nakladatelství Computer Press, 2002. s. 17

Ako je možné vidieť v týchto prípadoch, nejedná sa o prípady počítačovej kriminality, na ktoré sme v dnešnej dobe zvyknutí. Dôvodom je práve technická nevyspelosť.

2.3 Počítačový stredovek

12. augusta 1981 bol širokej verejnosti predstavený počítač typu IBM PC a začala sa tak úplne nová éra počítačov. Bol to rozmermi kompaktný a stavebnicovo usporiadaný typ počítača, ktorého tvar ho predurčoval na skoré rozšírenie medzi bežných užívateľov. Ostatne, aj skratka PC znamená *personal computer* a teda osobný počítač. Príchod tohto stroja priniesol revolúciu v používaní počítačov a taktiež aj v ponímaní kriminality v kyber priestore vzhľadom na to, že prepojenie počítačov pomocou modemov a telefónnych liniek na seba dlho čakať nemuselo. Vytvorením prvých *BBS (Bulletin Board System)* sa položili základy dnešného Internetu. Tento systém umožňoval vzájomnú komunikáciu medzi používateľmi, taktiež zdieľanie súborov, ale bola tu aj možnosť zapríčiniť škody vzdialenému užívateľovi.

Obdobie počítačového stredoveku je aj obdobie, kedy začali nastupovať aj rôzne typy počítačových vírusov. Najstarší spôsob infiltrácie je tzv. trójsky kôň. Ide o program, ktorý sa tváril ako užitočný, pričom v skutočnosti škodil. Prvý vírus nazvaný *Brain* sa vyskytol v roku 1986. Vytvorili ho dvaja bratia z Pakistanu – Basit a Farooq Alvi[9]. Tento vírus spôsobil niekoľko lokálnych „epidémií“. Neskôr, v roku 1988 študent Robert Morris, vypustil prvého prvý internetový vírus – červík. Tento červík sa kopíroval závratnou rýchlosťou a napadol približne šesť tisíc počítačov.

S postupom vývoja a s príchodom kompaktných diskov CD a taktiež s príchodom CD – ROM mechaník sa prudko zvýšila ďalšia časť počítačovej kriminality a to konkrétne počítačové pirátstvo. Po uvedení na trh mali CD – ROM mechaniky relatívne vysokú cenu, ale postupom času sa ich cena znižovala natoľko, že sa stala bežnou súčasťou vybavenia PC, a preto sa každý užívateľ mohol stať potenciálnym pirátom, a teda mohol páchať počítačovú kriminalitu. Takzvané „napaľovanie“ sa stalo doslova hitom, kde stačilo, aby mal jeden užívateľ originálny CD – ROM so software, hudbou, filmom alebo iným „know-how“ a pomocou vypálenia na iné CD takto mohol šíriť nelegálne obsah ďalej. V súčasnosti, v dobe rýchleho internetu, sa však vypaľovanie kompaktných diskov dostalo do úzadia. Pokiaľ chce užívateľ získať nelegálny software, stačí mu pár minút stráviť na internete, kde si konkrétnu vec vyhľadá a v priebehu pár sekúnd, či minút stiahne do svojho počítača.

[9] Hák, I. *Moderní počítačové viry*. s. 18, citované 5.5.2014, dostupné z http://lyceum-oajh.wz.cz/download/kniha_o_virech.pdf

2.4 Počítačový novovek

Pre počítačový novovek je charakteristické hlavne masové rozširovanie počítačov a to hlavne takých, ktoré fungovali pod operačným systémom Microsoft Windows. Dochádza aj k rozširovaniu siete Internet. Z akademických kruhov sa počítače a internet masovo rozširujú do domácností a začínajú byť obchodným nástrojom. Takéto obrovské rozšírenie počítačov a internetu viedlo k rozšíreniu kriminality v kybernetickom priestore, preto sa v tomto období postupne odohrávalo obrovské množstvo útokov, ktorých intenzita exponenciálne rástla.

Jedným z prvých prípadov kriminality v počítačovom novoveku bola kauza Citibank[10], kde skupina crackerov okolo ruského matematika Vladimíra Levina dokázala postupne banke ukradnúť viac ako 10 miliónov dolárov, ktoré si pripísali na svoj účet.

Ďalším mimoriadne známym prípadom bol prípad Intel[11], kde išlo o špionáž vykonanú nie hackermi alebo crackermi, ale vlastnými zamestnancami. Je bežné, že zamestnanci musia mať vo firme prístup k dôverným veciam. Najmä pokiaľ sú na vývojových pozíciach, prípadne na úrovni odborných pracovníkov. Práve v tomto prípade Guillermo Gaede, zamestnanec firmy Intel, okopíroval topografiu čipu Intel a poslal ho konkurenčnej firme. Táto konkurenčná firma zachovala mimoriadne eticky a upovedomila Intel o celej udalosti. Gaede bol nakoniec odsúdený na 33 mesiacov trestu odňatia slobody nepodmienečne.

Na intenzite nabrali rôzne útoky a vírusy na prelome tisícročí, teda od roku 1999 do 2001. Počas tohto obdobia sa vyskytlo mnoho známych internetových útokov, ktoré mal možnosť zaregistrovať aj bežný používateľ. Tieto vírusy však nenapádali tisíce počítačov ako tomu bolo napríklad v roku 1988, pri víruse od Morrisa, ale milióny resp. desiatky miliónov užívateľov. Najznámejšie vírusy boli napríklad *‚I Love You* a *‚Mellisa*. Tieto vírusy sa šírili pomocou e-mailov, ktoré mohol obdržať každý, kto mal vytvorenú e-mailovú schránku.

V prvom spomínanom víruse išlo o mail, ktorý sa maskoval za milostný list. Vírus bol natoľko deštrukčný a rozsiahly, že sa považuje za najničivejší na svete[12]. Prvý krát sa vyskytol 4. mája v roku 2000. Jeho autormi sú Filipínci Irene de Guzman, Onel de Guzman a Reomel Raomes. Počet napadnutých počítačov bol približne 45 miliónov, čo pri počte užívateľov pripojených na internet v roku 2000 predstavovalo približne jednu devätinu. Počet počítačov

[10]Matějka, M. *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 32
[11] Matějka, M. *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 33
[12] SCHMIDT, Charles a Tom DARBY. *The Morris Internet worm: The What, Why, and How of the 1988 Internet Wor* [online]. [cit. 2014-05-04]. Dostupné z: https://snowplow.org/tom/worm/worm.html 7.5.2013

pripojených na internet v roku 2000 bol približne 361 miliónov[13] všetkých „on-line“ užívateľov. Vírus sa šíril pomocou e-mailového klienta Microsoft Outlook. Po spustení sa automaticky rozposlal všetkým osobám uloženým v aplikácii. Vírus mal za úlohu v počítači vyhľadávať čísla a heslá ku kreditným kartám a automaticky ich zaslať tvorcom vírusu. Taktiež vírus upravil registre, pozmenil systémové súbory, odstranil rôzne typy súborov a súbory s koncovkami .mp3 nastavoval ako skryté. Vírus taktiež napadol napríklad Pentagon, CIA a britský parlament. Celkové škody sa odhadujú na 5,5 miliardy dolárov. Čo sa týka právnej dohry, autori boli na krátko, v máji roku 2000 zadržaní, avšak na Filipínach v tej dobe nebol k dispozícii žiadny zákon, ktorý by zakazoval šíriť *mallware.* Preto boli krátko po zadržaní všetci obvinení prepustení a taktiež bola stiahnutá obžaloba. Obvinenie so zneužívania kreditných kariet platilo naďalej.

Druhým menovaným bol vírus Mellisa, ktorý bol vytvorený Davidom L. Smithom[14] v roku 1999. Tento vírus sa rovnako ako vírus *I Love You*, šíril pomocou klienta Microsoft Outlook. Jeho princíp bol podobný, ako vo vyššie uvedenom prípade, a teda automaticky po infiltrácii sa rozposielal prvým 50 kontaktom. Nebol vytvorený za účelom deštrukcie, ale zahlcoval počítačové servery a spôsoboval problémy.

E-mailové vírusy neboli jedinou zbraňou počítačových kriminálnikov. Jednou z metód, ktorá sa používa dodnes je tzv. DoS (Denial of Service)[15] útok, teda odoprenie prístupu na server. Pri ňom sa útočník nesnaží infikovať cieľový počítač, ale opakovanými požiadavkami zahltiť server a dočasne ho vyradiť z činnosti. V súčasnosti rovnaké útoky vykonáva skupina hackerov a crackerov pod menom Anonymous.

Jedným z najnovších prírastkov do rodiny škodlivých *mallware* sa objavil koncom minulého roka a volá sa *TSPY_PIXSTEAL.A*[16]. Má za úlohu nájsť všetky fotografie na pevných diskoch, ktoré následne odošle na FTP server. Má však obmedzenie na 20 000 súborov. Možno sa to zdá zbytočné, kradnúť fotky, ale v dnešnej dobe, kde je fotoaparát bežnou súčasťou telefónov a tabletov, si ľudia fotia nielen zážitky, ale aj niektoré dôležité dokumenty ako napríklad zmluvy, rôzne projekty, prototypy, ktoré môže tvorca mallware zneužiť.

[13] ROYAL PINGDOM. *The incredible growth of the Internet since 2000* [online]. [cit. 2014-05-04]. Dostupné z: http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000/

[14] LEYDEN, J. THE REGISTER. *Melissa virus author jailed for 20 months* [online]. 2002 [cit. 2014-05-04]. Dostupné z: http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000/ 14.4.2014

[15] Matějka, M. *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 35

[16] VAVRO, P. PC.SK. *Nový malware kradne obrázky z počítačov* [online]. 2012 [cit. 2014-05-04]. Dostupné z: http://pc.zoznam.sk/novinka/novy-malware-kradne-obrazky-z-pocitacov 7.5.2013

Asi najnovším príspevkom do zbierky je mallware s názvom njRAT[17] pochádzajúci z Kuvajtu. njRAT sa šíri prostredníctvom externých diskov a umožňuje spúšťať rôzne príkazy, inštalovať ďalší mallware, zapisovať a meniť registre, zachytávať stlačenia klávesnice a taktiež vyhotovovať a sledovať snímky obrazovky. Zatiaľ je infikovaných približne „iba“ 24 000 užívateľov hlavne z blízkeho a stredného východu a severnej Afriky, ale aj z niektorých štátov Európy a USA

2.5 Základy počítačovej kriminality a jej definícia

Presne definovať počítačovú kriminalitu je v dnešnej dobe takmer nemožné. Príčinou je neustály a veľmi rýchly rozvoj informačných technológií, vďaka ktorému môžeme sledovať stále nové druhy a formy útokov. Nemôžeme si vystačiť s definíciou, v ktorej sa vraví, že počítačová kriminalita je protiprávne jednanie, ktoré má súvislosť s počítačom.

Pre porozumenie pojmu počítačová kriminalita je potrebné uviesť niekoľko zdrojov. Prvým je Trestný Zákonník, v ktorom sa počítačová kriminalita spomína ako prekonanie bezpečnostného opatrenia, neoprávnené získanie prístupu k počítačovému systému a jeho častiam. TZ taktiež pojednáva o neoprávnenom použití, vymazaní, poškodení, zničení a falšovaní dát, či už na nosiči alebo v systéme. § 230 rozoberá aj skutkovú podstatu trestného činu a teda úmysel vykonať inej osobe ujmu, prípadne obmedziť funkčnosť zariadenia alebo sebe neoprávnený prospech. Zákon sa zaoberá aj organizovanou skupinou

V Manuáli pre prevenciu a kontrolu počítačového zločinu OSN[18] je definované, že: „*Počítačová kriminalita predstavuje tradičné trestné aktivity ako napríklad krádež, podvod alebo falšovanie, teda skutky, ktoré sú trestné vo väčšine zemí na svete. K tomu sa pridružujú nové spôsoby zneužitia počítačov, ktoré sú, alebo by mali byť trestné.“*

Vo svojej práci tvrdí *Metonová*[19], že: "*Počítačová kriminalita je novým druhom závažnej trestnej činnosti v celosvetovom meradle v oblasti počítačových technológií. Od klasickej kriminality sa odlišuje celým radom osobitných charakteristík a zvláštností. Trestný čin môže byť*

[17] PRINCE, B. SECURITYWEEK. *'njRAT' Malware Gains Popularity Among Middle East Attack Groups* [online]. 2014 [cit. 2014-05-04]. Dostupné z: http://www.securityweek.com/njrat-malware-gains-popularity-among-middle-east-attack-groups

[18] *Manuál OSN pre prevenciu a kontrolu počítačového zločinu*, dostupné z: http://www.uncjin.org/Documents/EighthCongress.html.

[19] METONOVÁ, Z. *Počítačové právo* [online]. 2004 [cit. 2014-05-05]. Dostupné z: http://edi.fmph.uniba.sk/~winczer/SocialneAspekty/MetonovaPocitacovePravo.htm

spáchaný v priebehu niekoľko sekúnd bez toho, aby sa páchateľ nachádzal na mieste činu alebo poškodený zaregistroval spáchanie takéhoto trestného činu. Dokonca môže sa stať, že poškodený o spáchanom trestnom čine ani nevie. Trestná činnosť pomocou počítač alebo trestná činnosť spáchaná na počítačoch predstavuje veľké finančné straty, často presahuje hranice jedného štátu a stáva sa medzinárodným trestným činom. Vymedzením pojmu počítačová kriminalita sa zaoberali aj štáty EÚ. Príslušné výbory EÚ a EP sa dohodli na definícii počítačovej kriminality, podľa ktorej počítačová kriminalita je nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu".

Ak teda zhrnieme uvedené informácie, počítačová kriminalita je bežným protiprávnym javom až na to, že sa nemusí vykonávať priamo na mieste činu, ale stačí na to pohodlie domova a adekvátne vybavenie. Ako príklad môže poslúžiť nasledovná situácia. Pokiaľ chce niekto vykradnúť banku, musí prísť do inštitúcie osobne a hrubou silou, prípadne so zbraňou v ruke vymaniť peniaze od pracovníčky. No rovnako si môže sadnúť za počítač a svojimi schopnosťami a poznatkami dosiahne rovnaký výsledný efek. Takže termín počítačová kriminalita je síce relatívne mladý, ale zároveň je to iba nová možnosť, spôsob resp. zbraň, ako páchať kriminalitu, ktorá sa uskutočnuje už stáročia.

3 Formy počítačovej kriminality

Existuje veľa foriem počítačovej kriminality. Za posledných 30 rokov pribudlo mnoho druhov šírenia a vykonávania kriminality pomocou počítača. V nasledujúcej pasáži sa bude pojednávať o najznámejších a najpoužívanejších formách. Tieto formy budú zaradené do tried podľa Budapeštianskej dohody o počítačovej kriminalite.

3.1 Triedenie počítačovej kriminality

Pri definícii foriem sa stretávame s rovnakým problémom, ako pri definícii samotnej počítačovej kriminality. Poznáme veľa pohľadov na jej triedenie. Nepostačuje delenie na dva smery a to trestná činnosť páchaná proti počítaču a trestná činnosť páchaná s použitím počítača. Preto sa k týmto dvom kategóriám postupom času pridávajú ďalšie[20]:

1. úmyselné útoky voči vlastnému nosiču informácii,
2. počítač slúži ako prostriedok obohatenia, pričom sa ďalej rozlišuje,
   - krádež dát a programov,
   - krádež strojového času počítača,
   - nezákonná manipulácia s počítačom, dátami a programami.

Pri rozdeľovaní počítačovej kriminality sa môžu využiť aj poznatky doc. Smejkala[21], ktorý počítačovú kriminalitu rozdeľuje do dvoch kategórii :

1. Skutky, kde počítač, program, dáta, informačný systém a i. sú nástrojom trestnej činnosti páchateľa.
2. Skutky, kde počítač, program, dáta, informačný systém a i. sú cieľom útoku pričom môže ísť o tieto trestné činy:

   - fyzický alebo logický útok na počítač alebo komunikačné zariadenie,
   - neoprávnené používanie počítača alebo komunikačného zariadenia,
   - neoprávnené používanie alebo distribúciu počítačových programov,
   - zmenu v programoch a dátach,
   - neoprávnený prístup k dátam, získavanie utajovaných informácii,
   - trestné činy ktorých predmetom útoku je počítač ako vec hmotná.

[21] SMEJKAL, V. a i. *Počítačové právo*. Praha: C. H. Beck/SEVT 1995.

Jedným z najdôležitejších dokumentov ohľadne počítačovej kriminality je Budapeštianska dohoda o počítačovej kriminalite (Convention on Cybercrime)[22], ktorá bola podpísaná Českou Republikou 9.2.2005 a ratifikovaná bola 22.8.2013. Táto dohoda delí počítačovú kriminalitu na štyri oblasti:

1. **Trestné činy proti dôvere, integrite a dostupnosti počítačových dát a systémov, kam zaraďujeme:**
   - neoprávnený prístup,
   - neoprávnené odpočúvanie,
   - narúšanie dát,
   - narúšanie systémov,
   - zneužívanie zariadenia.

2. **Trestné činy vo vzťahu k počítaču**
   - počítačové falšovanie,
   - počítačový podvod.

3. **Trestné činy so vzťahom k obsahu počítača**
   - detská pornografia.

4. **Trestné činy so súvislosťou s porušovaním autorského práva a súvisiacich práv**

Štrasburský dodatkový protokol rozšíril tento okruh o štyri ďalšie skupiny xenofóbnych a rasových deliktov.

3.2 Jednotlivé formy počítačovej kriminality

3.2.1 Trestné činy proti dôvere, integrite a dostupnosti počítačových dát a systémov

1) Hacking - Je asi najstarším typom deliktu, ale v jeho počiatkoch sa ťažko mohol označovať za protiprávny. Definuje sa ako prenikanie do počítačového alebo riadiaceho systému inou, ako klasickou cestou. Napríklad prelomením ochrany. V začiatkoch hackingu nešlo o úmysel škodiť, ale skôr radosť a obdiv hackerskej spoločnosti. Hackeri boli začiatkoch programátori, ktorí sa vniknutím do programu snažili o jeho pochopenie, prípadne o jeho nápravu alebo vylepšenie.

[22] Convention on Cybercrime. Budapešť, 2004. Dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

S rastúcim vývojom informačných technológii sa hackeri začal deliť do dvoch hlavných kategórii a to, tí ktorí svojím konaním nemali záujem poškodiť cieľový program alebo systém a na tých, ktorí majú záujem o materiálne ciele a chcú pomocou hackingu škodiť. Existuje niekoľko typov hackerov[23].

- *Script Kiddies* alebo *Wannabes* – nachádzajú sa na najnižšej úrovni hackerského rebríčku. Bývajú označovaný ako tzv. *lammeri*. Ešte nižšie ako lammeri sú tzv. *loosers*. Podstatou Script Kiddies je v tom, že spúšťajú programy iných hackerov bez toho, aby im rozumeli. Jedná sa teda skôr o hru na hackerov, kedy samotní Script Kiddies ani úplne nevedia čo robia. Ostatnou hackerskou verejnosťou sú zatracovaní, avšak zákon ich stavia na rovnakú úroveň ako reálnych hackerov.

- *White Hats*, tiež označovaní ako *Ethical Hackers* – sú tzv. dobrí hackeri. Ich filozofiu a etiku môžeme prirovnať k pôvodným hackerom zo začiatku vývoja. Ak sa pokúšajú vniknúť do systému, robia to výlučne za účelom testovania a nachádzania chýb v systéme. Ich cieľom je lepšie zabezpečenie. Vo väčšine prípadov je to zo súhlasom majiteľa systému. Existuje aj skupina hackerov, ktorá si vraví *Samurajovia*. Ich podstata spočíva v tom, že sa najprv nabúrajú do systému a následne oboznámia správcu. Väčšinou pomocou anonymného emailu, v ktorom je popísaná chyba v systéme. Často sa s týmito hackermi môžeme stretnúť vo firmách na postoch analytikov, ktorí svoje služby poskytujú na profesionálnej úrovni. Môžu sa podieľať aj na zlepšovaní bezpečnosti formou aktualizácii, prípadne tvorbou zabezpečovacieho software tzv. antivírusov.

- *Black Hats* – Ide im väčšinou iba o ich osobný úžitok, či už finančný alebo majetkový. Sú úplným opakom White Hats. Ich činnosti sa môžu definovať ako protiprávny zásah do systému. Podieľajú sa na tvorbe škodlivého materiálu v podobe počítačových červov, vírusov, mallware, trójskych koní a pod. Títo hackeri bývajú často označovaní ako „H4H[24]“ a teda *Hackers for Hire*(Hacker na objednávku). Je to spojene s tým, že sú často najímaní rôznymi zločineckými skupinami.

- *Gray Hats* – Táto skupina hackerov sa pohybuje na hranici medzi dobrom a zlom, ako to z ich názvu (šedé klobúky) vyplýva. Definujú sa ako hackeri konajúci na vlastnú päsť. Vyhľadávajú teda chyby v systémoch s cieľom diskrétne na ne upozorniť správcu siete, prípadne majiteľa, za určitú finančnú odmenu. Nesnažia sa informácie zneužiť ako *Black Hats* a teda

[23] Matějka, M. *Počítačová kriminalita*. Praha : Vydavatelství a nakladatelství Computer Press, 2002, s. 54
[24] JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, 2007, s. 55

môžeme ich považovať za etickú časť hackerov. Na svoju činnosť však nemajú autorizáciu od konkrétneho majiteľa alebo správcu, čím konajú za hranicami zákona a týmto sú odlišní od *White Hats*. Ako bolo spomenuté, ich etika spočíva v tom, aby dosiahnuté informácie zdieľali s majiteľom a nemajú záujem o to, aby ich výsledky boli zneužívané inými hackermi. Istým spôsobom sa snažia, aby sa ukázali pred vývojármi, programátormi a takouto cestou chcú ponúkať svoje služby.

- Poslednou kategóriou, aspoň sú tzv. *Elite* alebo *3lit3* (v hackerskom slangu). Sú to hackeri, ktorí sa preslávili svojimi činmi, či už ako *Black*, *White* alebo *Grey* Hats. Sú tu ľudia typu Vladimíra Levina alebo partia okolo Irene Guzman z Filipín. Teda známi hackeri, ktorých útoky boli celosvetovo preslávené.

2) Sniffing[25] – z angl. čuchať. Zjednodušene sa môže povedať, že ide o odchytávanie resp. odpočúvanie komunikácie v počítačových sieťach osobou, ktorá nemá s touto komunikáciou nič spoločné. Na internete je voľne dostupných niekoľko desiatok *snifferov*. Umožňujú odchytávať konverzáciu a týmto nelegálnym spôsobom sa dostávajú k rôznym citlivým dátam, ako sú prístupové heslá a mená, čísla a kódy platobných kariet, znenie emailov a pod. Takto nadobudnuté informácie slúžia k prienikom do systémov a teda hackovaniu, prípadne slúžia na vydieranie a iné neoprávnené resp. trestné činnosti. Jedinou možnosťou ako sa voči sniffingu brániť je dôsledné šifrovanie komunikácie, resp. úplne zdržanie sa komunikácie s citlivými a osobnými informáciami.

3) Narúšanie dát – Typickým príkladom narúšania a zmeny dát je tzv. Cracking[26] – pri tejto metóde sa jedná o prelamovanie alebo obchádzanie ochranných prvkov elektronických alebo programových produktov, s následným neoprávneným používaním. Veľmi časté používanie crackingu je pri počítačových hrách. Jeden deň vyjde oficiálna hra na nosiči a v niektorých prípadoch je na druhý deň už jej čierna verzia na internete, zadarmo a nelegálne.

4) Veľmi častým príkladom narúšania dát je aj **vandalizmus** na webových stránkach, tzv. **web defacement**[27]. Jedná o útok a následnú zmenu vizuálnej charakteristiky web stránky. Cacker sa nabúra do servera a nahradí obsah web stránky svojim vlastným. Defacement sa označuje aj ako *elektronické grafity*. Tieto grafity sa stali pomerne rozšírené medzi partiou hackerov ktorí si vravia

[25] JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, 2007, s. 106
[26] JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, 2007, s. 106
[27] BRENNER, S. . *Cybercrime and the Law: Challenges, Issues, and Outcomes*. UPNE, 2012, s. 35

hackivists[28]. Jedná sa o spojenie dvoch slov *hack* – ako počítačový útok a *activism* ako aktivisti. Teda ľudia, ktorí sa snažia intenzívne presadiť svoje názory z určitých presvedčení napr. aktivisti za ľudské práva, aktivisti za slobodu zvierat a pod.

5) Narúšanie systému – do tejto kategórie spadajú kybernetické útoky a to hlavne tie, kde dochádza k závažnému narušeniu priebehu činnosti fungovania informačného systému. V tomto prípade sa jedná hlavne o tzv. DoS útoky. Skratka DoS značí vyradenie zo služby (z angl. Denial of Service) a ide o zaútočenie na spojovacie cesty k cieľovému stroju. To znamená, že tieto útoky sú zamerané na znemožnenie činnosti alebo poskytovania služby. Existuje niekoľko metód DoS útokov:

- zahltenie odosielaním zbytočných paketov[29] z viacerých zdrojov tzv. DDoS útok (Distributed Denial of Service), môže dosiahnuť až milióny útočiacich,
- zahltenie príkazom ping[30],
- zahltenie voľných systémových prostriedkov,
- DoS útoky môžu deliť na *lokálne* a teda, útočník môže mať prístup k počítaču na ktorý chce útočiť, alebo *vzdialené* útoky čo znamená, že nejaká chyba v systéme umožňuje napadnúť cieľový počítač bez potreby prístupu k cieľovému počítaču.

V popise nižšie sú uvedené najzákladnejšie varianty DoS útokov :

Mass mailing list – základy útoku spočívajú v tom, že sa zahltí určitá e-mailová schránka a tým sa vyradí z funkčnosti. Tento útok bol problémom hlavne v časoch, kedy bola veľkosť mailovej schránky obmedzená na niekoľko MB. V dnešnej dobe sú schránky niekoľko sto násobne väčšie, čiže útok už nie je tak častý. Priebeh spočíval v zaregistrovaní konkrétnej mailovej adresy na mnohých web stránkach s newslettermi, bulletinmi alebo aj pornografiou. To vyvolá zaplnenie schránky a nemožnosť prijímať nové správy. Útok je nebezpečný a hlavne ťažko vystopovateľný.

E-mail bombing – útok podobný mass mailing listu s rozdielom, že k vytvoreniu e-mailov sa využíva program. E-maily sú teda generované samotným útočníkom a záleží len na ňom, koľko ich pošle. Tento útok však nemusí viesť len ku zahlteniu e-mailového konta, ale tak isto aj o zahltenie celého poštového servera.

Malware – je definovaný ako časť škodlivého software, ktorý slúži a je využívaný útočníkmi na narušenie operácii počítača, zhromažďovanie citlivých informácii alebo k získaniu

[28] KRAPP, P. Terror and Play, or What Was Hacktivism?. *MIT Press Journals*. 2005, roč. 5, č. 19, s. 70-93. Dostupné z: http://www.mitpressjournals.org/doi/pdf/10.1162/152638105774539770
[29] Paket resp. pakety - bloky prenášaných dát
[30] Ping – preverenie funkčnosti spojenia medzi dvoma sieťovými rozhraniami do siete cieľového zdroja

prístupu do počítačového systému[31]. Malware zahŕňa keylogger, počítačový vírus, červika, trójskeho kona, spyware, adware a mnoho iných.

Vírusy – sú programy, ktoré sa môžu šíriť z počítača na počítač bez vedomia a väčšinou proti vôli užívateľa. Pomenovanie vírus je odvodený od schopnosti šíriť sa z nakazeného počítača na počítač, ktorý nie je dostatočne dobre chránený pred možnosťou nakaziť sa. Vírusy spôsobujú rôzne problémy. Od jednoduchého zaberania priestoru, cez tvorbu chýb v dôsledku ktorých sa bude systém spomaľovať až po nutnosť preinštalovania celého systému.

Prelamovanie hesiel – jeden z najstarších nástrojov používaný hackermi. Ako z jeho názvu vypovedá, slúži k prelomeniu určitého autorizačného hesla. Existujú dva typy útokov a to slovníkové útoky, kde program skúša použiť slová z vlastnej databázy alebo útoky hrubou silou, kde program postupne generuje všetky možné kombinácie potrebnej dĺžky. Rýchlosť prelamovania hesla záleží od výkonnosti počítača, type prelamovaného súboru, umiestnenia dát (pevný disk, sieť, internet) a štruktúre zakódovaného súboru. Pokiaľ by mal niekto ako heslo 4 veľké alebo malé písmená, ktoré sú ľubovoľne kombinovateľné, prelamovač hesla by sa k informáciám dostal za pár sekúnd. Pokiaľ by však užívateľ mal heslo s dĺžkou 8 znakov, kde by sa nachádzali aj číslice v ľubovoľnom poradí, prelamovanie hesla by mohlo trvať až 7 rokov. A pokiaľ by heslo malo pri rovnakých podmienkach 10 znakov, prelamovanie by zabralo neuveriteľných 26 984 rokov[32].

Červíky – sú programy, ktoré obsahujú škodlivý kód, napádajú hostiteľský počítač a využívajú jeho sieťové prepojenie na ďalšie šírenie do ostatných počítačov v sieti. Rozdiel medzi červíkom a vírusom je taký, že červík na rozdiel od vírusu nepotrebuje hostiteľský program na spustenie. Má v sebe zakomponované podprogramy ktoré zabezpečujú kopírovanie a jeho ďalšie šírenie. Poznáme dva typy červíkov:

- *E-mailový červík* – šíri sa pomocou zoznamu adries v e-mailovom klientovi. Na svoje šírenie používa komunikáciu pomocou e-mailov.
- *Sieťový červík* – červ sa šíri pomocou chýb v serverových častiach programov a sám nachádza a napáda servery vhodné na útok.

Spyware – je to škodlivý software, ktorý bez vedomia užívateľa pomocou počítača cez Internet odosiela dôverné informácie ako napríklad návštevnosť webových stránok.

---

[31] Oxford Dictionaries. [online]. [cit. 2014-04-30]. Dostupné z: http://www.oxforddictionaries.com/definition/english/malware

[32] JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, 2007, s. 63

Adware – býva väčšinou súčasťou voľne dostupného software. Po nainštalovaní takéhoto freeware, sa začnú užívateľovi zobrazovať rôzne reklamné ponuky. Podstatná časť adware spadá do šedej zóny, teda nie je škodlivý, ale môže obťažovať, napríklad zmenou štartovacej stránky internetového prehliadača

Backdoors – ako už z významu vyplýva, jedná sa o zadné vrátka, kde po inštalácii na cieľový počítač, je možné vzdialene riadenie napadnutého počítača. Pomocou takto napadnutého počítača hacker môže vykonávať nelegálnu činnosť bez toho aby bol priamo odhalený. Aj tu platí, že čím viacej napadnutých počítačov hacker „vlastní“, tým je väčšia šanca, že nebude odhalený.

Rootkit – je to súbor techník ktoré skrývajú činnosti prevádzané na operačnom systéme. Jedná sa o niečo podobné, ako pri Backdoors hackoch. Rozdiel je v tom, že rootkit je modifikovaný užívateľský program tak, aby administrátor napadnutého počítača nič nespoznal a hacker mal k prístroju neobmedzený prístup.

Trójsky kôň – jeden z najobľúbenejších nástrojov súčasnosti. Sú to malé programy - vírusy, ktoré sú zabalené do voľne stiahnuteľného obsahu. Po inštalácii stiahnutého súboru sa spolu s ním nainštaluje aj vírus, ktorý sa môže prejaviť hneď, ale aj postupom času.

Nástroje na prieskum siete – jedná sa o preskúmanie terénu pred začiatkom útoku. Mnoho potrebných informácii sa môže útočník dozvedieť z otvorených zdrojov cez bežný internetový prehliadač. Na stránkach firiem môže získať veľa potrebného materiálu a tým sa dostatočne dobre pripraviť na ofenzívu.

Kybernetické výpalné – podstata kybernetického výpalného spočíva v strachu z hrozby prieniku do spravovaného alebo vlastneného systému s prípadným zneužitím alebo zničením dát. Jedná sa teda o klasický delikt vydierania avšak pomocou modernej technológie.

Spamming – pod týmto pojmom sa skrýva posielanie nevyžiadanej elektronickej pošty. Väčšinou sa jedná o reklamný charakter. Spam je rovnako starý ako elektronická pošta sama. Existujú síce rôzne anti-spamové programy ktoré filtrujú správy, avšak k týmto programom majú prístup aj samotný spameri, takže si dokážu nájsť medzeru cez ktorú správy preniknú. Odhaduje sa, že podiel spamu na dnešnej e-mailovej komunikácii je približne 75%. To značí, že 3 zo 4 prijatých správ sú spamy.

3.2.2 Trestné činy so vzťahom k počítaču

Phishing – tento pojem znamená v preklade rybárčenie. V tomto význame lov na heslá a citlivé údaje užívateľov za účelom ich zneužitia. Jednou z najčastejších foriem je rozosielanie

podvodných e-mailov. V takomto e-maily sa podvodník vydáva za banku resp. finančnú inštitúciu a snaží sa klienta oklamať tým, že potrebuje overiť nejaké údaje a preto je nevyhnutné, aby sa adresát prihlásil cez priložený odkaz[33]. Príklad phishingu je uvedený v prílohách. Pokiaľ sa klient cez odkaz prihlási, útočník získa všetky potrebné údaje na to, aby mohol disponovať s účtom poškodeného. Jeden z posledných prípadov je z 10. mesiaca roku 2012 kedy bol klientom ČSOB rozoslaný e-mail o tom, že ich platba nemohla byť spracovaná resp. že platba nemôže byť dokončená. Následne sa mal klient prihlásiť cez uvedený odkaz a zadať svoje prístupové údaje[34].

Pharming – je v podstate podobný ako Phishing, ale omnoho nebezpečnejší. Metóda spočíva v hackovaní servera banky, ktorý má za účel priraďovanie doménových mien IP adresám tak, aby odkazoval na podvrhnuté stránky. Klient tak nemá šancu rozoznať podvrh. Následne všetko prebieha ako pri Phishingu a teda vykradnutie resp. zneužitie účtu obete.

Cyberstalking – jedná sa o spojenie dvoch slov. Stalking ako úmyselné prenasledovanie a obťažovanie inej osoby a cyber ako kybernetický teda počítačový alebo virtuálny. Cyberstalking je obťažovanie iných osôb pomocou počítača a kyberpriesotru. Páchateľ na to využíva väčšinou rôzne programy ako ICQ, Skype, MSN a rôzne chaty. Najčastejšími obeťami sú bývalí partneri, celebrity a iní.

Hoax – pod pojmom Hoax sa skrýva nevyžiadaná pošta resp. správa, ktorá obeť varuje pred nejakým vírusom, prosí o pomoc, informuje o nebezpečenstve alebo sa snaží pobaviť. Vo všeobecnosti však ide o zbytočné reťazové správy.

3.2.3 Trestné činy súvisiace s obsahom

Do tejto kategórie spadá najmä šírenie zakázaného alebo nelegálneho obsahu ako napríklad pornografia. Jej šírenie bolo známe aj pred masovým prepuknutím internetu, no možnosti boli dosť obmedzené. Kybernetický vek však priniesol nové možnosti čo porno priemysel využil naplno.

Nemenej závažným problémom ako pornografia, je aj šírenie extrémizmu. Asi všetky extrémistické skupiny sa snažia prezentovať svoj postoj a názory pomocou internetu. Informačné

[33] Slovenská sporiteľna: Príklady phishingu a pharmingu. [online]. [cit. 2014-05-05]. Dostupné z: http://www.slsp.sk/ActiveWeb/Page/sk/eb_phishing_pharming_priklady/priklady_phishingu_pharmingu.html 7.5.2013

[34] Hoax: CSOB nemuze spracovat vasi platbu. [online]. [cit. 2014-05-05]. Dostupné z: http://www.hoax.cz/phishing/csob-nemuze-zpracovat-vasi-platbu-20121011/

technológie odstránili mnoho komunikačných ťažkostí a sú masovo využívané aj ku komunikácii medzi jednotlivými časťami organizácii.

3.2.4 Trestné činy súvisiace porušovaním autorského práva a súvisiacich práv

Počítačové pirátstvo a **Warez** – pirátstvo a warez kráčajú spolu ruka v ruke. Počítačoví piráti boli čiastočné popísaní už pri historickom delení, teda budú opísaní v skratke. Ide o neoprávnené používanie počítačových programov a súčastí počítačových programov takým spôsobom, ktorý patrí výlučne autorovi alebo inému nositeľovi autorského práva. Pod túto kategóriu spadá používanie a šírenie software, zneužívanie hudobných súborov, plagiátorstvo, nelegálne nakladanie s multimédiami a iné. Warez je určitý druh počítačového slangu označujúci autorské diela s ktorými je nakladané v rozpore s autorským právom. Väčšinou pomocou zdieľania dát vďaka FTP serverom a Peer – to – Peer sieťach. Rozdiel medzi pirátstvom a warezom je v tom, že piráti sa snažia nelegálny software finančne zneužiť a teda vytvoria nelegálnu kópiu originálneho nosiča, ktorý vyzerá legálne a snažia sa ho speňažiť. Warez resp. warezové skupiny tento software prípadne multimédia sprístupňujú zadarmo buď horeuvedenými metódami, alebo pomocou webových stránok. Financie na svoj chod získavajú z reklamy umiestenej na svojich web stránkach.

Cybersquatting – táto metóda je už na ústupe, ale v časoch rozmachu internetu, kedy veľké spoločnosti iba spoznávali internet, to bola celkom rozšírená metóda. Jednalo sa o zaregistrovanie webovej stránky s menom veľkej spoločnosti. Na stránke je následne umiestnená reklama na odpredanie stránky. Prípadne sa môže jednať o zaregistrovanie domény s veľmi podobným menom ako cieľová firma a následne parazitovanie. Jeden verejne známy prípad sa udial v Českej Republike a to konkrétne s doménou bankovnipoplatky.com resp. bankovni-poplatky.com.

4 Sociálny hacking

Sociálny hacking je aktuálnou témou, ktorá prevláda v počítačovom svete. Internet je natoľko rozšírený, anonymný a zároveň previazaný, že užívatelia nemajú možnosť zistiť, kto ich sleduje, kto zneužíva ich osobné dáta, kto si prezerá ich históriu prehliadača web stránok a kto má k týmto údajom prístup. Stačí jedno tlačidlo „Like“ v prostredí Facebooku na stránku so zdravou výživou a e-mailová schránka sa postupne začne zapĺňať poštou od rôznych portálov, ktoré sa zaoberajú zdravým stravovaním. Nejedná sa len o Facebook alebo internet ako taký. Sociálny hacking sa môže prevádzať aj cez telefón. Stačí napísať správu ktorá bude obsahovať podozrivé slová ako napríklad: „BOMBOVÝ zápas, náš tým vyhral 3:0.“, a je možné, že budete mať pri vstupe do USA problém s tajnou službou.

4.1 Úvod do sociálneho hackingu

Na úvod treba podotknúť, že samotný pojem sociálny hacking nie je priamo definovaný v žiadnej literatúre a ani na internete. Významovo najbližšie je k tomuto slovnému spojeniu termín *sociálne inžinierstvo*. Tento druh inžinierstva spočíva v pochopení umenia manipulovania s ľuďmi a následným zneužitím ich osobných informácii za pomoci získania dôvery od subjektu[35]. Pri sociálnom hackingu však o žiadnu dôveru nejde. Je to zneužívanie dát bez akejkoľvek možnosti ovplyvniť únik, spracovanie a zneužitie privátnych informácii.

Sociálny hacking by mal byť podľa Budapeštianskej dohody zaradený do prvej kategórie, a teda Trestné činy proti dôvere, integrite a dostupnosti počítačových dát a systémov. Čo to vlastne sociálny hacking je? Ako sa môže definovať?

Ako sa niekoľko krát v tejto práci spomínalo hack resp. hacking je úmyselné nabúranie sa druhou osobou do systému užívateľovho počítača, bez jeho vedomia a zneužívanie jeho osobných údajov, ktoré má jedinec uložené vo svojom počítači. V tomto prípade sa termín systém musí bližšie špecifikovať, lebo naň môžeme nahliadať z viacerých uhlov pohľadu.

Systém môže byť vnímaný z klasického počítačového pohľadu ako program, ktorý spravuje zdroje počítača a poskytuje rozhranie na prístup k týmto zdrojom. Ale na pojem systém sa môže hľadieť aj z etymologického uhla. V gréčtine *sýstéma* značí členitý celok, zložený

[35] Symantec: Social Engineering Fundamentals, Part I: Hacker Tactics. [online]. [cit. 2014-05-05]. Dostupné z: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

z viacerých častí[36]. Presne takýto členitý celok sú údaje ktoré má jedinec uložené v podobne fotiek, statusov, uložených e-mailov a inej komunikácie na serveroch rôznych sociálnych sietí, cloudových serveroch, na e-mailových kontrách a pod. Sú to určité údaje a informácie, ktoré človek produkuje a ukladá si počas svojho života. Mnohokrát znamenajú veľmi veľa pre konkrétnu osobu a taktiež sú neuveriteľne cenné rovnako, ako v prípade počítačového systému.

Nejedná sa síce o súbory nevyhnuté pre život jedinca, ale môže sa jednať o rôzne fotografie určené len pre vyvolených, dôležité pracovné dokumenty, prístupové heslá a pod. Čiže rovnako ako počítač, aj človek má svoj „virtuálny" systém, ktorý nie je nevyhnutý na jeho život, ale nenásilne ho núti aby si založil konto na sociálnych sieťach, mal e-mailové konto, komunikoval s ostatnými pomocou rôznych internetových komunikačných prostriedkov a i. A presne toto je systém, ktorý sa pri sociálnom hackingu napáda.

Sociálny hacking by mal byť definovaný, ako neoprávnené manipulovanie s osobnými dátami za účelom ich zneužitia a využitia. Prečo by mal niekto záujem o privátne informácie, ktoré nemusia mať žiadnu cenu? Niekedy ide o to, že sa hacker resp. cracker dostane k dôležitým dátam, ako napríklad čísla a heslá účtov, platobných kariet, citlivých osobných údajov a i., ktoré môžu byť následne zneužité a môžu slúžiť na vydieranie. Taktiež niektoré celosvetovo známe spoločnosti majú eminentný záujem o to, aby sa dostali k informáciám ohľadne vašej on-line aktivity a histórie vášho internetového prehliadača. Avšak v dnešnej dobe kedy štátne mocnosti chcú mať všetko pod kontrolou a monitorovať každého a všetko, sa môže stať, že bude jedinec hacknutý jednotlivými štátnymi zložkami a ich bezpečnostnými alebo informačnými službami. Či už pre podozrenie z nekalej činnosti alebo iba tak. Pre istotu.

4.2 Zneužívanie osobných údajov

Sociálny hacking však nie je pojem, ktorý by spadal iba do tohto desaťročia. O sociálnom hackingu ako takom, sa môže hovoriť už niekoľko desaťročí. Počiatky má niekde v rozšírení telefonických liniek do domácností a s tým spojené telefonické reklamy. Asi typickým príkladom zneužívania osobných dát je, keď niekoľko krát do týždňa zvoní telefón s rôznymi reklamnými ponukami. Prečo mnoho používateľov internetu nachádza preplnenú poštovú schránku rôznymi letákmi, reklamnými ponukami? Odkiaľ majú tieto agentúry telefónne čísla, adresy bydliska, prípadne e-mailové adresy na zasielanie reklamnej pošty?

[36] OXFORD DICTIONARIES. *Definition of System* [online]. [cit. 2014-05-05]. Dostupné z: http://www.oxforddictionaries.com/definition/english/system 14. 4. 2014

Mnoho informácii človek vystaví dobrovoľne okoliu pomocou svojho Facebook profilu, kde ukazuje ostatným, často krát úplne neznámym ľudom, s kým sa priatelí, kde býva, kam chodí na školu príp. kde pracuje, telefónne číslo, adresu bydliska a mnoho iného. Je pravdou, že mnohé z týchto údajov jedinec nemusí zverejniť. Je to na jeho uvážení, či chce aby ostatní videli jeho osobné údaje. Facebook však nie je jediným zdrojom na čerpanie osobných dát.

Ďalším z prípadov, kde sa ľudia dobrovoľne vzdávajú osobných údajov ako je meno, adresa, číslo a e-mail je registrovanie sa v rôznych obchodoch, ktoré využívajú klubové karty alebo vernostné programy. Obchodník ponúkne neuveriteľnú ponuku ktorá spočíva v zľave pár percent pri nákupe alebo postupné zbieranie kreditu, ktoré znamená zľavu na tovar registrovaným klientom, ktorí sú ochotní vymeniť takýto štýl zľavy za svoje súkromie.

Registrácia v obchodných reťazcoch, alebo predajniach a s tým spojené klubové karty súvisia s prijatím antispamového zákonu, ktorý sa vzťahuje na neoprávnené zasielanie obchodných ponúk. Zákon totiž upravuje zodpovednosť, práva a povinnosti osôb, ktoré poskytujú služby a šíria obchodné oznámenia. A to predovšetkým prostredníctvom e-mailu, mobilného telefónu alebo pevnej linky. Zákon definuje obchodné oznámenia, ako všetky formy oznámenia určené k priamej alebo nepriamej podpore tovaru, služieb alebo image podniku fyzickej či právnickej osoby. Pokiaľ teda fyzická alebo právnická osoba získa od svojho zákazníka podrobnosti o jeho elektronickom kontakte v súvislosti s predajom výrobku alebo služby podľa požiadavkou ochrany osobných údajov, môže táto osoba využiť tieto podrobnosti elektronického kontaktu pre potreby šírenia obchodných oznámení týkajúcich sa ich vlastných výrobkov alebo služieb, za predpokladu, že zákazník má jasnú a zreteľnú možnosť jednoduchým spôsobom zadarmo, prípadne na účet fyzickej alebo právnickej osoby odmietnuť súhlas s takýmto využívaním svojho elektronického kontaktu[37]. Zákazník sa teda môže rozhodnúť, či má alebo nemá záujem o registráciu a následné zasielanie pošty. Často je však takáto registrácia spojená s určitými výhodami, preto zákazník neváha vzdať sa svojich údajov.

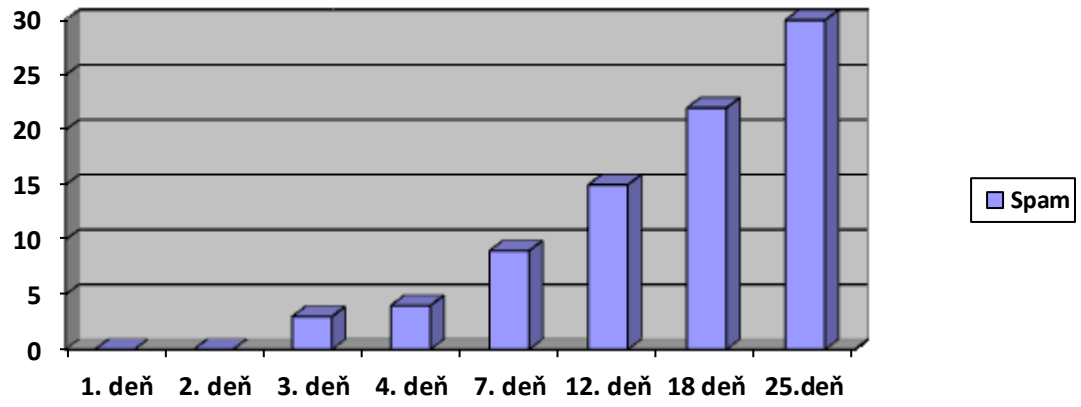
V neposlednom rade je tu asi najznámejšia spoločnosť na svete, ktorá prevádzkuje nielen internetový vyhľadávač zvaný Google ale aj mnoho iného. Tento „veľký brat“ monitoruje pohyb na internete, zisťuje čo konkrétny človek vyhľadáva a zbiera osobné údaje. Spoločnosť Google taktiež prevádzkuje aj jeden z najväčších e-mailových serverov G-mail. Je teda počudovania hodné, že keď sa v jeden deň snažíme nájsť pomocou vyhľadávača vhodnú dovolenku, na druhý deň nám príde niekoľko e-mailov s reklamami na dovolenky a hotely v rôznych destináciách

[37] Zákon č. 480/2004 Sb., v znení neskorších predpisov

Autorova skúsenosť z posledných dní je taká, že na internete pomocou vyhľadávača Google, vyhľadával jeden automobil značky Subaru. Po pár dňoch sa automaticky na rôznych internetových stránkach začali spomínané automobily zobrazovať prostredníctvom reklamy. Predtým, keď tento druh auta nevyhľadával, sa podobné reklamy zamerané na spomínaný automobil nezobrazovali.

V rámci výskumu bola založená fiktívna emailová adresu, za účelom získania relevantných dát. Adresa bola zaregistrovaná na rôznych webových portáloch. Prvé dni po založení konta, bola emailová adresa neaktívna. Počet nevyžiadanej pošty – spamu – bol nulový. Postupne sa začal emailový účet registrovať na viacerých domácich a zahraničných serveroch. Zo začiatku sa schránka zapĺňala iba pomaly, so stúpajúcou intenzitou registrácii však rapídne stúpal aj počet nevyžiadanej pošty, až v priebehu jedného dňa dosiahol počet 30.

Graf 1: Počet nevyžiadanej pošty



Zdroj: spracované autorom na základe vlastných dát z výskumu

Google nesleduje len pohyb na internete, ale aj život ľudí. Služba Google Earth má zmapovanú celú planétu. Samozrejme, že táto udalosť sa nepáčila mnohým svetovým veľmociam, preto môžeme pri prezeraní zeme pomocou Google Earth naraziť na rôzne utajené miesta, ktoré musel Google odstrániť alebo ukryť[38].

Ale to nestačilo a tak pomocou služby Street View zmapoval všetky vyspelé štáty sveta, ich mestá, ulice a nazhromažďoval pritom nepovolené informácie. Nešlo len o nevhodné zábery, išlo hlavne o nabúranie sa do Wi-Fi sietí rôznych používateľov. Google to najprv

[38] SWITCHED. *51 Places You're Not Supposed to See on Google Maps* [online]. 2008 [cit. 2014-05-05]. Dostupné z: http://www.switched.com/2008/07/16/things-you-cant-see-on-google-maps/

odôvodnil tým, že chcel zachytiť informácie o Wi-Fi sieťach, ktoré neskôr môže použiť k lokalizácii užívateľov a k poskytovaniu lokalizačných služieb. Neskôr sa objavili informácie, že sa spoločnosť dostala aj k samotným údajom prenášaných pomocou nezabezpečených bezdátových sietí. Google tak nazhromaždil obsahy e-mailov, textových správ, hesiel, rôzne histórie internetových prehliadačov a ostatné citlivé dáta[39].

Google sa oficiálne priznal k zhromaždeniu dát, až keď sa celá udalosť dostala pred súd. Snažil sa však naťahovať pojednávanie čo najdlhšie. Nakoniec súd dospel k rozhodnutiu, že pokuta vo výške 25 tisíc USD bude adekvátna. Pri čistom zisku v roku 2012 ktorý činil 10,74 miliardy dolárov[40] to nie je ani len tisícina percenta. Nejednalo sa však o jedinú pokutu pre spoločnosť. Pre ďalší nepovolený zber dát službou Street View, zaplatí tento krát spoločnosť 7 miliónov dolárov. V auguste 2012 Google zaplatil rekordnú pokutu vo výške 22,5 milióna dolárov za to, že potajomky sledoval milióny užívateľov webu[41]. V posledných mesiacoch dostal Google ďalšiu pokutu vo výške 145 tisíc EUR od Nemeckého mesta Hamburg. Pokuta bola pre systematické a nezákonné zhromažďovanie údajov pri službe Street View[42]. Hamburgská agentúra pre ochranu dát a slobodu informácii bola prvá, ktorá odhalila Google pri zbere dát z Wi-Fi routerov v Nemecku. Agentúra 22.4.2013 vyhlásila, že Google sa priznal k zberu dát vrátane e-mailov, hesiel, fotografii a komunikácie na chatoch v rokoch 2008 až 2010 pri príprave spustenia služby Street View. Na svoju obhajobu Google uviedol, že celá zbierka bola neúmyselná a bola výsledkom programátorskej chyby. To ako niekto pri mapovaní ulíc „náhodne“ a „neúmyselne“ ukradne chúlostivé dáta z verejných Wi-Fi routrov však neozrejmil. Preto nad celou obhajobou visí pomyselný otáznik.

Pokuta v takejto výške je pre spoločnosť Google smiešnou. Momentálna legislatíva EÚ ale neumožňuje dať vyššiu pokutu, ako 150 tisíc EUR. V najbližšej dobe sa plánuje zmena zákonov, kde budú sankcie a právne dopady omnoho tvrdšie. V tomto prípade by Google mohol dostať pokutu vo výške 2% ročného obratu spoločnosti, čo by činilo niečo okolo jednej miliardy

[39] Federal Communications Commission. *Notice of apparent liability for forfeiture* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://transition.fcc.gov/DA-12-592A1.pdf

[40] ŠPELINA, M. BYZNISPLAC.CZ. *Společnost Google vykázala rekordní zisk* [online]. 2013 [cit. 2014-05-05]. Dostupné z: http://byznysplac.cz/spolecnost-google-vykazala-rekordni-zisk/ /

[41] FARRELL, C. FEDERAL TRADE COMMISION. *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

[42] HAMBURG COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION. *Fine imposed upon Google* [online]. 2013 [cit. 2014-05-05]. Dostupné z: https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2013-04-22_Google-Wifi-Scanning.pdf

dolárov[43]. Nepredpokladá sa však, že pripravované zmeny budú účinné skôr, ako za niekoľko rokov, preto je momentálne zbytočné zaoberať sa týmito skutočnosťami.

Počítač však nie je jediným zdrojom na zbieranie informácii tejto spoločnosti. Google ma dosah aj na inteligentné telefóny s operačným systémom Android. Počas písania SMS správ, sa môže dostať k detailom o dostupných Wi-Fi sieťach, dozvedieť sa komu je správa určená, a veľmi presne určiť polohu jedinca.

Čo presne môže zo surfovania po sieti resp. z používania telefónu, tabletu a počítača Google zistiť? Informácii je hneď niekoľko[44]:

- jazyk ktorý používate,
- s kým komunikujete on-line,
- detaily o zariadení s ktorým ste pripojený na sieť (počítač, tablet, mobilný telefón) – rozlíšenie displeja, jazyková verzia operačného systému, miesto odkiaľ sa pripájate – presnosť na metre,
- údaje o konkurenčnom software, ktorý vlastníte,
- hľadané výrazy,
- detaily o hovoroch, správach, mailoch,
- IP adresu,
- vašu polohu,
- dostupné Wi-Fi vysielače a mobilné vysielače vo vašom okolí.

Ako sa dá zamedziť sledovaniu, zhromažďovaniu a zneužívaniu osobných dát týmto gigantom? Riešení je hneď niekoľko, ale sú to lokálne riešenia pre jedincov, ale nie pre spoločnosť.

Ako prvé riešenie sa ponúka úplne Google ignorovať a používať iné vyhľadávacie stránky, ktoré sú podobne úspešne vo vyhľadávaní. Nie je však zaručené, že iný vyhľadávač nebude taktiež zhromažďovať údaje. Ďalšou možnosťou sú rôzne programy ktoré zabezpečia súkromie počas surfovania po sieti. Robia to pomocou skrývania a anonymizovania IP adresy a šifrovania všetkej internetovej komunikácie. Ďalej sú možnosti v rôznych aplikáciách ktoré blokujú pokusy

[43] FARIVAR, C. ARS TECHNICA. *Proposed EU law would have hit Google with nearly $1 billion in fines* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://arstechnica.com/business/2012/04/proposed-eu-law-would-have-hit-google-with-nearly-1b-in-fines/

[44] PACULÍK, M. TECHSME.SK. *Čo o vás Google vie a načo mu to je* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://tech.sme.sk/c/6240422/co-o-vas-google-vie-a-naco-mu-to-je.html

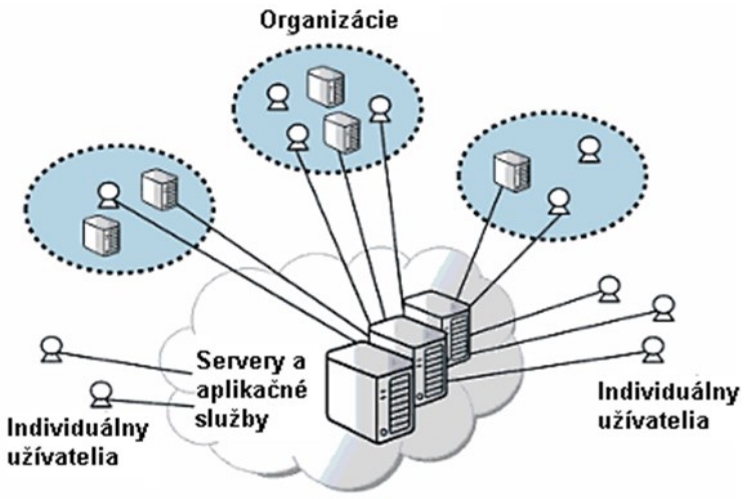
o sledovanie užívateľa. Namierené sú hlavne proti prvkom Google Analytics. V neposlednom rade je tu možnosť zakázania akýchkoľvek skript na stránkach, v tom prípadne však človek nebude mať možnosť pozerať videá, používať platformu Flash a i.

Samozrejme Google nie je jediná spoločnosť, ktorá zneužíva návštevníkov svojich web stránok. Existujú internetoví obchodníci, ktorí keď zistia, že ich webová stránka bola otvorená pomocou nejakého produktu od firmy Apple – či už iPhone alebo iPad – automaticky zdvihnú pre takýchto zákazníkov ceny. Je to spôsobené tým, že produkty s logom odhryznutého jablka sú všeobecne známe ako drahšie a exkluzívnejšie, za ktoré je ochotný spotrebiteľ zaplatiť vyššiu sumu. Nemá tak problém s tým, aby zaplatil aj vyššiu cenu za ponúkaný produkt, ktorý momentálne na webe hľadá.

4.3 Problém cloud computeringu a cloudových serverov

Cloud computering je nový model vývoja a používania rôznych podnikových aplikácii, sofrwarových platforiem a hardverových infraštruktúr, cez ktorý pristupuje užívateľ pomocou internetového prehliadača. Podstata cloudu spočíva v tom, že dáta sú uložené na externých serveroch konkrétnych cloudových spoločností a používateľ má možnosť k ním pristupovať z akéhokoľvek zariadenia. Pre bližšiu špecifikáciu je priložený obr. č. 1

Obr. č. 1 - Schéma cloudu



Zdroj: Harding, Ch. *CloudComputingfor Business: TheOpenGroupGuide*. Dostupné z: ttp://www.opengroup.org/sites/default/files/contentimages/Press/Excerpts/first_30_pages.pdf

Úspech cloudu spočíva v tom, že užívateľ nemusí vynakladať financie na nákup, údržbu a starostlivosť o hardware . V tomto prípade úložný hardware ako harddisky, CD resp. DVD-rom, USB kľúče a pod. Zaplatí si určitý objem dát na serveri, ktorý následne môže zapĺňať ľubovoľným obsahom.

Výhody cloudu:

- nízke náklady na prevádzku – používateľ platí iba za služby ktoré využíva,
- väčšia mobilita – prístup k firemným informáciám z akéhokoľvek miesta a zariadenia s internetom,
- flexibilita – umožňuje dynamicky reagovať na zmeny,
- spoľahlivosť a bezpečnosť – dáta sú uložené na externých zariadeniach a pravidelne zálohované.

Nevýhody ktoré sú spojené s cloudovými servermi sa už tak ľahko na internete neuvádzajú. Spoločnosti sa snažia nalákať záujemcov na znížené náklady, menšiu starostlivosť a väčšiu bezpečnosť.Väčšou mobilitou sa snažia prevádzkovatelia nalákať tých ľudí, ktorí sú on – line často. Vždy ale nastanú situácie, kedy jednoducho prístup k internetu nemusí byť samozrejmý. Preto je omnoho jednoduchšie mať dáta uložené na prenosnom médiu a tým pádom budú stále dostupné. Pri firmách je možnosť zriadenia VPN servera, s ktorým sa dá komunikovať bez problémov z ktoréhokoľvek miesta s prístupom na internet, takže nie je dôvod na to, aby si niekto musel pracovné veci zdieľať pomocou cloudu.

Najdôležitejšou témou je spoľahlivosť a bezpečnosť. Tu je niekoľko vyjadrení cloudových spoločností ohľadne bezpečnosti osobných dát. *Dropbox*[45]: „*Pri používaní našich služieb nám poskytujete informácie, súbory a priečinky, ktoré poskytujete službe Dropbox (ďalej len „váš obsah“). Váš obsah je vašim plným vlastníctvom. Nebudeme si uplatňovať vlastníctvo na žiadny váš obsah. Tieto podmienky nám neposkytujú žiadne práva na váš obsah, alebo vaše duševné vlastníctvo, s výnimkou obmedzených práv, ktoré sú potrebné na spustenie služby ako je popísané nižšie.“*

[45] ŠMODRK, Z. MÔJANDROID.SK. *Podmienky použitia služieb spoločnosti Google by mohli odradiť od používania Google Drive* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.mojandroid.sk/2012/04/30/podmienky-pouzitia-sluzieb-spolocnosti-google-by-mohli-odradit-od-pouzivania-google-drive/

SkyDrive[46]: „*S výnimkou materiálov, ktoré vám poskytujeme s našou licenciou, si neuplatňujeme nárok na vlastníctvo obsahu, ktorý prevádzkujete prostredníctvom našich služieb. Váš obsah je vašim vlastníctvom. Taktiež nekontrolujeme, neoverujeme a ani neschvaľujeme obsah, ktorý vy a ostatní sprístupňujete prostredníctvom našej služby.*"

Nakoniec pripájam vyjadrenie spoločnosti Google[47] a ich názoru na ich cloud *Drive*: „*Keď do našich Služieb nahráte alebo inak poskytnete obsah spoločnosti Google (a osobám, s ktorými spolupracujeme) tým udeľujete celosvetovú licenciu na používanie, hostovanie, uchovávanie, reprodukciu, úpravu, vytváranie odvodených diel (ako sú diela, ktoré vzniknú následkom prekladu, úpravy či iných zmien, ktoré uskutočníme s cieľom dosiahnutia lepšej integrácie vášho obsahu do našich Služieb), sprístupnenie, zverejnenie, verejné vykonávanie, verejné zobrazenie a distribúciu takéhoto obsahu.*"

Tým sa Google nepriamo priznal k budúcemu prezeraniu osobných dát a k ich prípadnej úprave a vlastníctvu. V skratke, pokiaľ niečo nahráte na servery od Google Drive , strácate akýkoľvek dohľad nad svojim dátami a taktiež aj ich vlastníctvom. A stále to nie je to najhoršie. Spoločnosti síce tvrdia že dbajú na bezpečnosť a stabilitu ich serverov, ale ako je známe z histórie, žiaden ochranný systém nie je neprekonateľný. Môže sa stať, že skupina hackerov napadne serveri spoločností prevádzkujúcich cloud a odcudzí dáta používateľom. Prípadne môže vyradiť z činnosti serveri, ktoré majú za úlohu uchovávať dáta. Tým pádom užívateľ príde dočasne, alebo úplne o všetky svoje informácie nahrané pomocou cloud computeringu. Samozrejme, to isté sa môže stať aj na osobnom počítači, ale v tom prípade nesiete zodpovednosť sami za seba. Keď sa však stane problém a cloudová spoločnosť príde o vaše dáta, nenesie zodpovednosť nikto. Nemáte žiadnu možnosť vyvodiť dôsledky voči takejto spoločnosti za stratu alebo prípadný únik osobných údajov.

Vzhľadom na §64 odsek 12 zákona o telekomunikáciách[48] v ktorom sa vraví nasledovné : „*Pokud službu bylo možno využít jen částečně, anebo ji nebylo možno využít vůbec pro závadu technického nebo provozního charakteru na straně poskytovatele veřejné telekomunikační služby, je tento povinen zajistit odstranění závady a přiměřeně snížit cenu nebo po dohodě s účastníkem zajistit poskytnutí služby náhradním způsobem. Poskytovatel veřejné telekomunikační služby není*

[46] ŠMODRK, Z. MÔJANDROID.SK. *Podmienky použitia služieb spoločnosti Google by mohli odradiť od používania Google Drive* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.mojandroid.sk/2012/04/30/podmienky-pouzitia-sluzieb-spolocnosti-google-by-mohli-odradit-od-pouzivania-google-drive/

[47] ŠMONDRK, Z. MÔJ ANDROID. *Podmienky použitia služieb spoločnosti Google by mohli odradiť od používania Google Drive* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.mojandroid.sk/2012/04/30/podmienky-pouzitia-sluzieb-spolocnosti-google-by-mohli-odradit-od-pouzivania-google-drive/

[48] Zákon č. 127/2005 S.b, v znení neskorších predpisov

povinen uhrazovat jejím uživatelům náhradu škody v důsledku neposkytnutí služby nebo vadného poskytnutí služby.“

To znamená, že firma nenesie zodpovednosť za výpadok služby a teda nemusí hradiť škody za vzniknutý výpadok. Pokiaľ má firma na cloudovom serveri uložené dáta ktoré súrne potrebujete odoslať dodávateľovi, odberateľovi alebo nejakému inému obchodnému partnerovi a server je nedostupný, v následku čoho dostane pokutu alebo príde o zákazku, škodu uhradí zo svojich vlastných zdrojov.

V prospech tohto tvrdenia vraví aj prieskum spoločnosti Trend Micro[49] z roku 2011, kde až 43% opýtaných podnikov zažilo bezpečnostné problémy s poskytovateľmi cloud služieb. Prieskum sa konal na vzorke 1200 odborníkov z IT, ktorí pracujú vo firmách s viacej ako 500 zamestnancami. Účastníci prieskumu pochádzali z USA, Veľkej Británie, Nemecka, Indie, Kanady a Japonska.

Nastáva preto otázka, za akým účelom je celý systém cloud computeringu vytvorený. Je tu snaha spoločnosti pomôcť zákazníkom a za poplatky im ponúkať neobmedzený virtuálny priestor? Nie je náhodou virtuálny úložný priestor iba zámienkou k tomu aby bol prístup k osobným dátam jednoduchší ako tomu bolo doteraz? Kto vlastne stojí za týmito spoločnosťami?

4.4 Monitorovanie ľudí štátom a bezpečnostnými zložkami

Ako bolo v úvode tejto kapitoly spomínané, stačí sa niekedy nevhodne vyjadriť do telefónu prostredníctvom SMS správy alebo telefónneho rozhovoru a môžete sa stať záujmovou osobou pre niektoré štátne bezpečnostné zložky. Taktiež stačí, aby sa jedinec nevhodne zachovali tam, kde na neho môže mať dohľad priemyselná kamera, ktorú prevádzkuje polícia, prípadne aby odoslal e-mail ktorý môže mať citlivý charakter a je v hľadáčiku. Ako je vlastne možné takýmto spôsobom kontrolovať neuveriteľné množstvo audiovizuálnych prípadne textových dát? Odpoveď je jednoduchá. INDECT.

Na úvod treba spomenúť správu parlamentného kontrolného výboru z Bundestagu[50], ktorá dobrovoľne odhaľuje rozsah bežného a teda oficiálneho sledovania resp. odpočúvania. V roku 2010 analyzovala Nemecká federálna spravodajská služba a ďalšie orgány asi 37 miliónov e-mailov, hovorov a faxov, s cieľom vystopovať teroristov a prípadných pašerákov. Hľadanie pozostávalo z približne 15 tisíc kľúčových slov, ako *raketa*, *bomba*, *atóm* a prípadných názvov

[49] SUBRAMANIAN, K. TREND MICRO INC. *Public Clouds* [online]. 2011 [cit. 2014-05-05]. Dostupné z: http://la.trendmicro.com/media/wp/public-clouds-whitepaper-en.pdf
[50] *CHIP: Proč jsem PODEZŘELÝ*. Praha: CHIP Holding G.m.b.H, 2012, roč. 22, č. 10, s. 40-43

zbraní. Teda je možné, že pokiaľ sa niekto zmienil v e-maile o bombovom atletickom mítingu, kde pretekár vyštartoval ako guľka z pištole, Nemecká vláda by komunikáciu vyhodnotila ako nebezpečnú.

Pokiaľ však človek nepácha trestnú činnosť, vo svojej podstate by mal byť s takýmto riešením spokojný. Otázkou je, či je ochotný vzdať sa dosť veľkej časti súkromia kvôli sledovaniu možných teroristov a nebezpečných živlov. Tu je namieste použiť citát Benjamina Franklina : „ *Tí, ktorí sú ochotní obetovať slobodu za dočasnú bezpečnosť, si nezaslúžia ani slobodu, ani bezpečnosť.“*.

Pri zvážení, že z celkovej množiny približne 37 miliónov rôznych zozbieraných dát bolo len 213[51] relevantných a z toho bolo dvanásť e-mailov, vyplýva , že úspešnosť tejto akcie je 1,7 nebezpečného e-mailu alebo telefonátu k 10 000 zozbieraným osobným údajom. Otázkou teda ostáva, nakoľko je takýto hon za sledovaním bezpečnosti výhodný. Napriek tomu ho štát ešte dotuje, vylepšuje a rozširuje.

Čo vlastne projekt INDECT znamená? Je to skratka z *Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Enviromental* a teda inteligentný informačný systém podporujúci pozorovanie, vyhľadávanie a detekciu pre bezpečnosť obyvateľov v mestskom prostredí. Inak je to výskumný projekt v oblasti inteligentných bezpečnostných systémov vykonávaný niektorými štátmi Európskej Únie[52]. Konkrétne je v tomto projekte zapojených 10 členských štátov. Nechýba medzi nimi ani Česká Republika. Zároveň aj celá rada partnerských organizácii. Tieto organizácie dostali dotáciu od Európskej Únie vo výške 10,9 milióna EUR. Peniaze využijú na vývoj platformy pre systém, ktorý bude dohliadať a zhromažďovať dáta pomocou mikrofónov, kamier alebo špeciálnych snímačov. Zo získaných informácii bude INDECT spoznávať podozrivé správanie alebo násilie.

V rámci tohto projektu sa pripravuje aj vývoj integrovaného centrálneho systému, ktorý podporuje aktivity polície. Všetko končí pri vývoji súboru techník, ktoré podporujú sledovanie prostriedkov na internete, analyzujú získané informácie a spoznávajú kriminálne aktivity a hrozby. Projekt je koordinovaný z univerzity v Krakove. V Českej Republike je do systému INDECT zapojená naša VŠB-TUO, Katedra telekomunikačnej techniky.

Ako vlastne bude systém fungovať? Hlavné slovo v tomto prípade bude mať počítač. Jednotlivé zábery z kamier sa nedostanú do rúk vyšetrovateľom. Je to software, ktorý vyhľadáva potenciálne nebezpečných ľudí, prípadne hroziace nebezpečenstvo. Tu však nastáva jeden

[51] *Proč jsem PODEZŘELÝ*. Praha: CHIP Holding G.m.b.H, 2012, roč. 22, č. 10, s. 40-43
[52] INDECT. *Welcome to Indect* [online]. 2008 [cit. 2014-05-05]. Dostupné z: http://www.indect-project.eu/

problém. Podľa čoho systém určí, aké chovanie je v norme a ktoré chovanie znamená potenciálne nebezpečenstvo? Polícia na základe každodenných udalostí definovala abnormálne správanie, ktoré v systéme INDECT slúži ako základ pre identifikáciu chovania. Medzi podozrivé chovanie preto patrí napríklad behanie, dlhé sedenie na jednom mieste, položenie batožiny na zem, sedenie na podlahe v autobuse alebo vo vlaku, nadávanie na verejnosti, stretávanie sa s väčšou skupinou ľudí a podobné záležitosti, ktoré vo svojej podstate neznamenajú nič zlé.

Vynárajú sa rôzne názory špecialistov, ktorí vravia, že systém v súčasnosti prakticky nemôže odhaliť abnormálne správanie sa jednotlivca. Pri veľkej skupine alebo dave ľudí je to predvídateľný jav, ale nie pri jedincovi samotnom. Nie je totiž možné presne definovať ako sa jedinec v určitých situáciách zachová. Taktiež si umelá inteligencia môže pomýliť dieťa na pleciach rodiča za batoh a môže dotyčnú osobu začať monitorovať. Bez nejakého dôvodu, iba pre chybu rozpoznávania sa rodič s dieťaťom môže stať hrozbou pre „veľkého brata“.

Výhodou v nevýhode takéhoto sledovacieho systému je to, že počítač nemá predsudky. Preto si všíma aj tých ľudí ktorí by bežnému človeku možno unikli. Počítaču ale chýba ľudské myslenie a preto sa zameriava na každého tou istou mierkou. Rovnako si bude všímať desať ročného chlapca aj 25 ročného muža s nožom v ruke. Taktiež nedokáže adekvátne rozhodovať o potenciálnej hrozbe. Ako napríklad keď sú dvaja muži sú na letisku. Jeden si odloží svoj kufor a ide na toaletu kým druhý muž kufor pohľadom stráži. Človek by takéto správanie akceptoval, systém v tom však vidí nebezpečenstvo.

Aké sú predpokladané výsledky INDECT-u? Oficiálne verzie vravia o niekoľkých výsledkoch, a to konkrétne:

- skúšobná inštalácia systému sledovania a dohľadu v metropolitnej oblasti,
- počítačový systém, ktorý bude schopný získavať a inteligentne spracovávať dáta,
- zariadenie pre mobilné sledovanie objektov,
- vyhľadávače pre rýchlu detekciu a sémantické hľadanie osôb,
- systém sledovania trestnej činnosti na internete,
- sledovanie osobného života ľudí a špehovanie v záujme vlády.

Najhlavnejším z týchto bodov je posledný. Teda sledovanie osobného života ľudí a špehovanie v záujme vlády. Je jasné, že štát chce mať pod kontrolou svojich obyvateľov a zároveň mať pod kontrolou bezpečnosť. Strata súkromia je ale dosť veľká daň. Ešte k tomu, keď človek nemá istotu ako sa s jeho osobnými bude zaobchádzať. Zároveň nevie, či náhodou údaje,

ktoré boli zozbierané nebudú ukradnuté pri systematickom útoku skupiny hackerov. Zároveň je na uváženie legislatívna stránka problému, lebo ani štát nemá právo na to, aby špehoval svojich obyvateľov bez povolenia a dôvodu. Nastáva tu taktiež otázka toho, ako sa bude môcť človek očistiť, pokiaľ ho systém zaradí do zložky „potenciálna hrozba“ a bude k nemu napríklad vyslaná motorizovaná zložka policajného zboru na kontrolu.

Zostáva nám otázka, prečo štáty a ich bezpečnostné zložky chcú a neustále vyvíjajú rôzne metódy na ochranu obyvateľstva, keď v konečnom dôsledku nie je zaručené, že takýto systém bude fungovať a slúžiť správne.

4.5 Facebook a jeho pozadie

Od roku 2004, kedy táto sociálna sieť vznikla až do dnes sa na Facebooku zaregistrovalo a trvalo ho využíva vyše jednej miliardy ľudí[53]. Z čísel vyplýva, že najviac užívateľov je z USA (135 miliónov), Indie (43,5 milióna) a Mexika (32 miliónov). V Českej republike tomuto fenoménu prepadlo približne 3,6 milióna ľudí, čo je asi 34% celej populácie. Na obr. č. 2 máme percentuálne zastúpenie kontinentov na používaní Facebooku.

Obr. 1 - Používatelia Facebooku

Zdroj: DIGITAL STRATEGY CONSULTING. *Facebook hits 1bn users* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.digitalstrategyconsulting.com/intelligence/2012/10/facebook_hits_1bn_users_top_re.php

[53] STATISTIC BRAIN. *Facebook Statistics* [online]. 2014 [cit. 2014-05-05]. Dostupné z: http://www.statisticbrain.com/facebook-statistics/

Nepochybne je teda najväčšou súkromnou zbernicou ľudských dát na svete. Či ide o fotografie, ktorých bolo za 9 rokov fungovania siete nahraných vyše 21 miliárd, vyjadrené názoroy a pod. Kto však stojí za celou touto zbernicou dát? Z čoho bol projekt zo začiatku financovaný?

História siaha do apríla 2006, kedy spoločnosť Facebook dostala finančnú podporu vo výške 27 miliónov dolárov z rôznych zdrojov, medzi ktoré patrí aj spoločnosť Greylock Partners. Táto spoločnosť je štvrtým najväčším akcionárom sociálnej siete viď. graf 1. Investičná firma Greylock Partners investovala taktiež aj do Instagramu, spomínaného Dropbpoxu a iných.

Graf 2 - Kto vlastní Facebook

Zdroj: *CHIP: Tajné síly na INTERNETU*.

Jedným z najskúsenejších zamestnancov Greylock Partners je istý *Howard E. Cox*, ktorý sa vo svojej oblasti pohybuje cez 40 rokov. Počas nich zastával v spoločnosti niekoľko riaditeľských postov. Howard Cox nie je iba investor, ale má pomerne blízko aj k politike. Pred príchodom do Greylock Partners pracoval v kancelárii amerického ministerstva obrany a do roku 2009 sedel v obchodnej rade Pentagonu. Howard E. Cox je však aj členom správnej rady manažérov

spoločnosti *In-Q-Tel*. Táto spoločnosť je niečo ako investičné rameno CIA, ktorá bola založená touto spravodajskou službou[54].

CIA cez In-Q-Tel podporuje napríklad aj Google Earth. Samotná spoločnosť In-Q-Tel sa ani netají tým, že má záujem o sledovanie osobných údajov. Veď priamo v brožúrke sa môžeme dočítať o tom, že: „Sledovanie sociálnych médií je nevyhnutnou súčasťou pre vlády, pokiaľ si chcú udržať rastúce politické hnutie[55]“. To znamená, že vláda resp. vlády nechcú byť prekvapené prípadnou facebookovou revolúciou, ako v prípade tzv. Arabskej jari, ktorá začala na konci roku 2010 a trvá dodnes. Pri tejto revolúcii sociálne média zohrali veľmi veľkú rolu.

Aby však niekto mohol sledovať také veľké množstvo dát za deň, potrebuje na to špeciálny software, ktorý by dokázal cielene analyzovať nazhromaždené údaje. Za týmto účelom CIA taktiež učinila strategické investície. Firma Palantir Technologies, taktiež financovaná skupinou In-Q-Tel, takýto software momentálne vyrába. Palantir sa dokonca verejne pomocou reklamy k podobnému software priznáva.

4.6 Cenzúra a snaha o kontrolu nad internetom

V decembri roku 2012 sa uskutočnila konferencia WCIT – 12, kde sa mal prediskutovať a schváliť nový medzinárodný telekomunikačný predpis. Vystupovali tu dve hlavne protichodné skupiny: *ICAAN* - The Internet Corporation for Assigned Names and Numbers a teda internetové združenie pre prideľovanie mien a čísel a *ITU* – The International Telecommunication Union v preklade Medzinárodná telekomunikačná únia. Snaha ICAAN bola v tom, aby mohol internet organizovane a nerušenie rásť, zatiaľ čo ITU mala v záujme regulovať internet. Na strane ITU sa nachádzali štáty ako Čína, Rusko a aj niektoré arabské štáty ako Egypt, Alžírsko, SAE a iné, pričom všetci mali záujem o tzv. znárodnenie internetu. V prílohe je obr. 4, kde sú zobrazené členské štáty, ktoré hlasovali za návrh (označený zelenou farbou) a štáty ktoré boli proti (označené bielou farbou). Pridávam konkrétnu citáciu návrhu: „*Členské země budou mít svrchované právo stanovovat a implementovat pravidla v oblasti šíření a správy Internetu, včetně mezinárodních pravidel, a regulovat národní segmenty Internetu, stejně jako aktivity poskytovatelů (operating agencies) poskytujících přístup k Internetu či přenášejících internetový provoz*.“[56]

[54] *CHIP: Tajné síly na INTERNETU*. Praha: CHIP Holding G.m.b.H, 2013, roč. 23, č. 2, s. 36-38
[55] *CHIP: Tajné síly na INTERNETU*. Praha: CHIP Holding G.m.b.H, 2013, roč. 23, č. 2, s. 36-38
[56]INTERNATIONAL TELECOMMUNICATION UNION. *World Conference on International Telecommunications* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

V prílohe na obr. 5 je možné vidieť, nakoľko je internet regulovaný a cenzurovaný štátmi v dnešnej dobe.

Návrhy neprešli, ale zároveň nevyhrala ani jedna strana. Nakoniec sa prijali niektoré návrhy, ktoré dávajú štátom väčšiu právomoc. Nie však takú fatálnu, ako to bolo uvedené v prvom prípade. Taktiež sa neschválil nový medzinárodný telekomunikačný predpis, jeho prijatie a schválenie sa odložilo.

Z tohto však máme možnosť vidieť , že niektoré štáty majú eminentný záujem o kontrolu dát, ktoré sú ich občanom k dostupnosti a taktiež chcú mať kontrolu nad tým, čo sa pomocou internetu šíri. Pokiaľ by návrh prešiel, je možné, že štát začne plne reguloval obsah internetu. To by znamenalo, že v konkrétnej krajine, by mali ľudia prístup iba k informáciám, ktoré prešli cenzúrou a sú neškodné. Taktiež by sa mohlo stať, že štát by v takomto prípade mohol internet zdaniť, aby sa mohol dostať k novým príjmom do štátnej pokladnice. Je možné, že pri snahe o takéto výrazné zmeny, internet ako ho poznáme teraz, tu už onedlho nebude.

5 Ekonomické a právne dopady sociálneho hackingu a počítačovej kriminality.

Počítačová kriminalita spolu so sociálnym hackingom majú mnohokrát nevyčísliteľnú resp. veľmi ťažko vyčísliteľnú ekonomickú hodnotu. Dôvodov je hneď niekoľko. Poškodený jedinec si ani nemusí byť vedomý toho, že z jeho účtu odchádzajú mesačne minimálne čiastky na cudzí účet, nedokáže presne oceniť údaje, o ktoré prišiel pri infikovaní počítača vírusom, nevie , že jeho osobné údaje sú predávané a pod. Z právneho hľadiska je často ťažké dokázať a usvedčiť konkrétnu osobu zo spáchanie deliktu, či už kvôli dokázaniu úmyslu, alebo aj kvôli samotnému usvedčeniu páchateľa.

5.1 Právne dopady počítačovej kriminality a sociálního hackingu

Táto podkapitola je venovaná konkrétnym zákonom, ktoré bojujú voči počítačovej kriminalite a svojim spôsobom aj proti sociálnemu hackingu. Mnoho zákonov, ktoré sa využívajú pri počítačovej kriminalite sú zakotvené už dávno, len s tým rozdielom, že páchateľ skutok vykonáva pomocou počítača a nie osobne.

V momentálnej legislatíve je pojem hacking zadefinovaný a to konkrétne v § 230 Trestného zákonníka (ďalej len TrZ).

„(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací, b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné

majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2 a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny b) způsobí-li takovým činem značnou škodu c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán, c) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo d) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.[57]“

V ods. jedna je chránená dôvernosť počítačových dát a počítačového systému. Počítačový systém je chránený pred ohrozením jeho bezpečnosti. Až následné sú chránené integrita a dostupnosť počítačových dát a systémov.

V ods. dva sa naopak primárne ochraňujú integrita a dostupnosť počítačových dát a systémov. Ochrana je poskytovaná počítačovým dátam a počítačovým programom pred neoprávnenými zásahmi, ktoré by mohli mať vplyv na existenciu, kvalitu, správnosť dát a chráni pred neoprávneným používaním uložených počítačových dát.

Bez postihu však môže obísť hacker, ktorého aktivita bude viesť k testovaniu bezpečnostného systému a bude prevádzaná na základe tvorcovej resp. majiteľovej požiadavky.

V § 231 TrZ sa pojednáva o ochrane spoločnosti a ľudí pred možnosťou ohrozenia vyplývajúcou z nekontrolovateľného nadobudnutia a prechovávania zariadení, nástrojov a prostriedkov, ktoré primárne slúžia ku spáchaniu trestných činov porušenia tajomstva dopravovaných správ podľa § 182 odst. 1 písm. b), c) alebo neoprávneného prístupu k počítačovému systému a nosiču informácii podľa § 230 odst. 1. 2.

Predmetom §232 TrZ je ochrana dát a technického, prípadne programového vybavenia počítača. Kriminalizuje aj niektoré nedbalostné zásahy do nosičov dát a vybavenia počítača, prípadne iného technického zariadenia pre spracovávanie dát. Kriminalizácia nedbalej formy je

[57] Zákon č. 40/ 2009 Sb. v znení neskorších predpisov

však značne diskutabilná, preto sa trestná zodpovednosť obmedzila na hrubú nedbalosť a spôsobenie značnej škody,.

Pri počítačovom pirátstve a vytváraniu nelegálnych kópii sa môže taktiež využiť § 268 TrZ, ktorý vraví o porušení práv k ochrannej známke. Tento skutok je častý najmä pri počítačovom pirátstve, kedy páchateľ vytvorí legálne vyzerajúcu kópiu nosiča s úmyslom ju predať, pričom na to nemá oprávnenie.

§ 270 TrZ pojednáva o porušení autorských práv, práv súvisiacich s právom autorským a práv k databáze. Za predmet ochrany ako autorské dielo sa považuje podľa zákona aj počítačový program, ak je autorovým duševným výtvorom. Za počítačový program sa považuje nehmotný výsledok autorovej činnosti. Pri tomto zákone je dôležité to, že oproti trestnému zákonu spred roku 2010 dochádza k určitému uvoľneniu napätia ohľadne warezu. Na základe tohto ustanovenia budú postihovaní tí páchatelia, ktorí svojím jednaním spôsobujú značné škody tzn. škody väčšie ako 500 000 Kč. Toto je celosvetový trend, kedy pri porovnávaní spôsobenej škody a nákladov na stíhanie, bude zahajované trestné stíhanie iba pri vyššej spoločenskej nebezpečnosti.

§ 272 TrZ, ktorý hovorí o všeobecnom ohrození sa za určitých podmienok môže vzťahovať napríklad na útok na navigačný systém lietadla alebo iné systémy na ktorých sú závislé ľudské životy alebo ich zdravie.

§ 276 TrZ sa zaoberá poškodzovaním a ohrozením prevádzky všeobecne prospešného zariadenia a teda zahŕňa aj problematikou nielen tzv. DoS útokov, kedy sa snažia hackeri o znefunkčnenie prevádzky či už internetového pripojenia alebo určitého serveru.

§ 290 TrZ hovorí o získaní kontroly nad vzdušným dopravným prostriedkom, civilným plavidlom a pevnou plošinou. V dnešnej dobe kedy sa do lietadlového systému dá nabúrať aj pomocou telefónu, ako to prezentoval bezpečnostný konzultant *Hugo Teso* na fóre v Amsterdame[58], ktorý dokázal pomocou smart-phone so systémom Android vniknúť do lietadlového palubného počítača a v režime autopilot dokázal s lietadlom manipulovať, je tento zákon použiteľný aj na prípady počítačovej kriminality.

Problematike spammingu sa venuje § 11 zákona č. 480/2004 Sb., o niektorých službách informačnej spoločnosti. Zaoberá sa hromadným alebo opakovaným šírením obchodných ponúk pomocou elektronický prostriedkov.

[58] HYCLÁK, E. SVET.IT. *Androidová aplikácia sa dokáže nabúrať do palubného systému lietadla* [online]. 2013 [cit. 2014-05-05]. Dostupné z: http://www.svetit.sk/2013/04/androidova-aplikacia-sa-dokaze-naburat-do-palubneho-systemu-lietadla/

S rastúcim rozvojom informačných technológií sa mnoho trestných činov prenieslo z osobnej formy na neosobnú. Príkladom toho je tzv. „kyberšikana“. Samotná šikana síce nenapĺňa skutkovú podstatu trestného činu, avšak zahŕňa v sebe znaky niektorých iných trestných činov ako napríklad Obmedzovanie osobnej slobody (§171TrZ), Vydieranie (§ 175TrZ), Utláčanie (§ 177 TrZ), často spojené aj s trestnými činmi Ohovárania (§184 TrZ). Kyberšikana je realizovaná prostredníctvom informačných a komunikačných technológií (internetu, mobilných telefónov, tabletov) k aktivitám, ktoré majú dané osoby dlhodobo obťažovať, ohovárať, ponižovať, urážať, vydierať alebo inak vyvádzať z rovnováhy a stresovať ich s cieľom im ublížiť. S nástupom sociálnych sietí, ktoré v tomto smere ponúkajú neobmedzené možnosti, naberá kyberšikana úplne iný rozmer.

Pri sociálnom hackingu je preukázateľnosť skutku podstatne ťažšia. Jednak z toho dôvodu, že jedinec si ani nemusí byť vedomý zneužitia osobných dát resp. nemá možnosť zistiť, že niekto jeho osobné dáta zneužil, pokiaľ nejde o trestné činy spojené s krádežou napr. vykradnutie bankového konta.

Taktiež sa ťažko dokazuje zneužívanie dát rôznymi súkromnými spoločnosťami prípadne štátnymi spravodajskými službami. Pokiaľ by však došlo k alternatíve, že by jedinec nepopierateľne preukázal odcudzenie osobných dát, ďalej by sa postupovalo podľa hore uvedených paragrafov.

5.2 Ekonomické dopady počítačovej kriminality a sociálneho hackingu

Každoročne spôsobuje počítačová kriminalita a taktiež aj sociálne hackovanie miliardové škody. Zo správy o počítačovej kriminalite z roku 2011[59] môžeme zistiť, že obete počítačovej kriminality ročne prídu o približne 388 miliárd USD. Do tejto správy bolo 24 štátov. Z Európy to boli : Belgicko, Dánsko, Nemecko, Španielsko, Francúzsko, Taliansko, Holandsko, Poľsko, Švédsko, Švajčiarsko a Spojené Kráľovstvo. Len v USA za rok 2013 došlo k stratám približne 100 miliárd USD a k stratám resp. nevytvoreniam 500 000 pracovných miest. Z množiny 24 krajín sa škody odhadujú na približne 500 miliárd USD za rok 2013. A teda platí, že počítačová kriminalita je vysokozisková forma trestnej činnosti s relatívne nízkym rizikom, ktorá je stále bežnejšia a čím ďalej tým viac nebezpečnejšia.

Spomenutá suma však nie je a nemôže byť presným vyčíslením straty, ktorú prináša nelegálna práca s výpočtovou technikou. Dôvodov je hneď niekoľko. Firma ktorá prišla o svoje

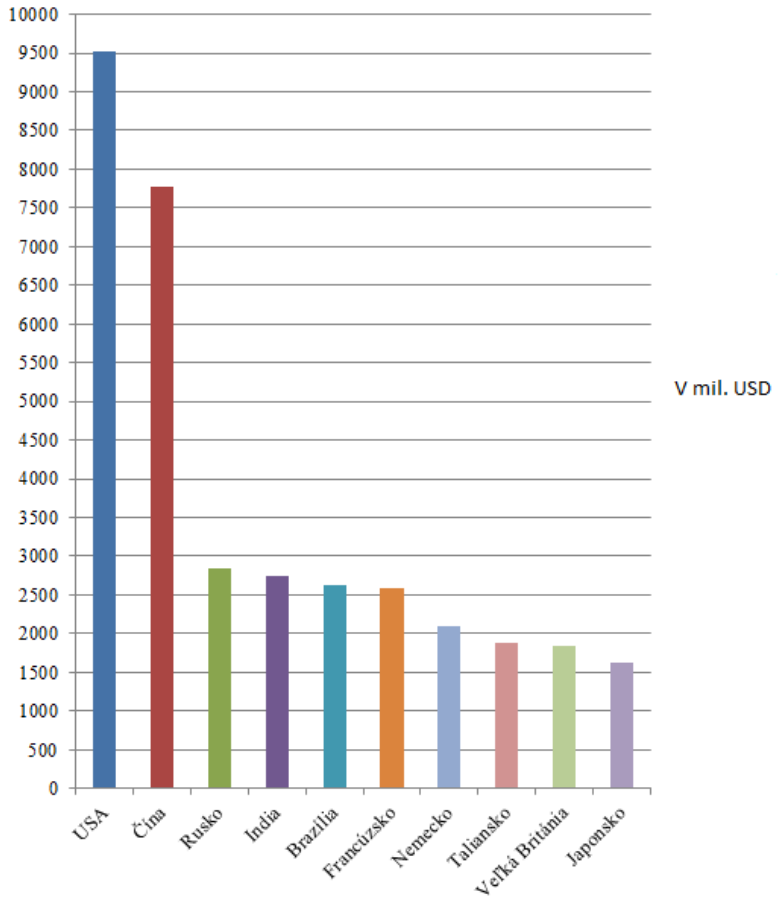
[59] NORTON. *Cybercrime report 2011* [online]. 2012 [cit. 2014-05-05]. Dostupné z: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf.

dáta vďaka útoku hackerov, len ťažko môže vyčísliť hodnotu ich práce a prípadných stratených údajov. Človek ktorého dáta boli odcudzené, si pri istej dávke šikovnosti hackerov ani nemusí všimnúť, že mesačne z jeho účtu odíde nejaké euro alebo dolár niekam preč. Len ťažko budeme finančne ohodnocovať stratu osobných dát, ktoré sa vymažú vplyvom nejakého počítačového vírusu. Dôvodov prečo sa nedá tento druh kriminality presne finančne ohodnotiť je však omnoho viac. Preto sa v tejto časti pokúsim zamerať sa na druhy počítačovej kriminality, ktorá má relatívne presné údaje.

5.2.1 Počítačové pirátstvo

Takmer polovica celosvetovo používaného software tvoria pirátske resp. nelegálne kópie. Odhaduje sa, že pokiaľ by sa miera pirátstva znížila o 10% prinesie to asi143 miliárd dolárov zisku a vytvorí približne 500 000 nových pracovných miest. Celkovo sa strata v dôsledku pirátskeho kopírovania pohybuje okolo 59 miliárd dolárov ročne na celom svete. V grafe č. 2 môžeme vidieť odhadované straty z počítačového pirátstva v rôznych krajinách sveta.

Graf 3 - Odhadované straty v dôsledku pirátskeho kopírovania



Zdroj: Spracované autorom na základe dát z *Norton Cybercrime report 2011*

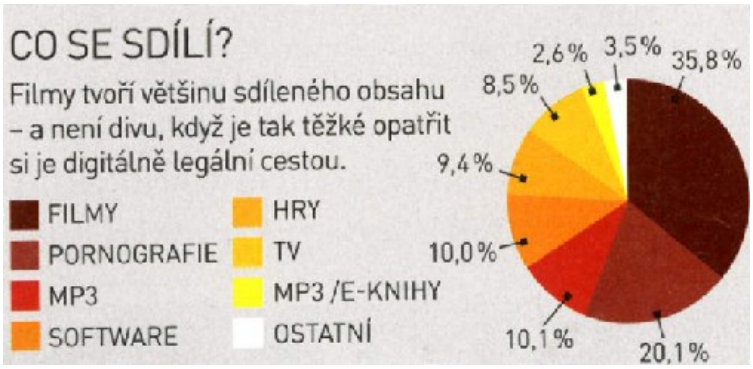
Obr. 3 - Pirátstvo v číslach - Porovnanie s rokom 2010

Zdroj: CHIP: Pirátvstí v číslech.

Na uvedenom obrázku 3 môžeme vidieť, že množstvo nelegálneho obsahu na internete v roku 2010 v porovnaní s rokom 2005 stúplo významne hlavne v oblasti hier. Dá sa to vysvetliť hlavne stúpajúcou tendenciou vývoja hier a taktiež ich následného uvedenia do predaja. V porovnaní s filmami a knihami sú hry oveľa zaujímavejším artiklom na pôde softwarového pirátstva aj vzhľadom na ceny pri uvádzaní produktov na trh.

Na grafe 4 je možné vidieť percenuálne zloženie zdielaného nelegálneho obsahu na internete. Filmy spolu s pornografiou tvoria viac ako polovicu pirátskeho obsahu. Je to spôsobené horšou dostupnosťou a mnohokrát aj znemožnením nákupu takéhoto diela cez internet. Filmy sa dostávajú na DVD/Bluray nosiče značne neskôr, ako sú uvedené v kinách. To častokrát núti používateľov zaobstarať si takýto produkt nelegálnou cestou.

Graf 4 - Obsah zdielaných dát na internete



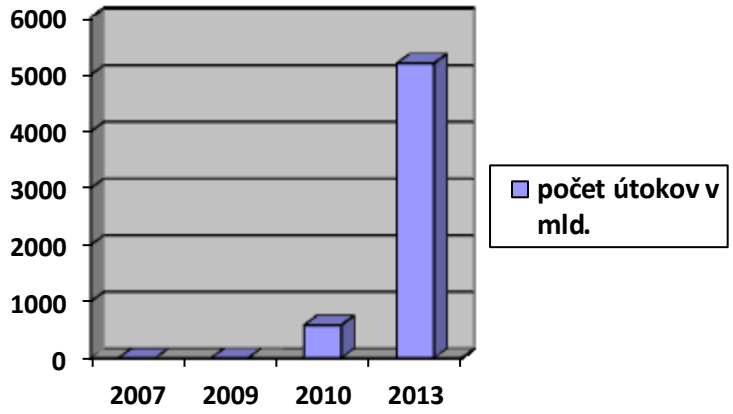
Zdroj: CHIP: Pirátvstí v číslech.

5.3 Porovnanie počtu napadnutých používateľov internetu za poslednú dekádu

Internet sa stal najväčším fenoménom za posledné dekády. Za 10 rokov sa zvýšil počet používateľov internetu takmer 4 násobne[60]. Zatiaľ čo v máji roku 2004 bol približný počet používateľov okolo 740 miliónov, v marci roku 2014 to bolo približne 2.9 miliardy osôb. Takýto rapídny nárast a dopad na počítačovú kriminalitu je samozrejmý. Zo štatistiky ktorú zverejnila spoločnosť Kaspersky Secutity zaoberajúca sa vývojom antivírových programov, vyplýva, že v roku 2007 bolo zaznamenaných približne 24 miliónov útokov proti používateľom Kaspersky Security[61]. V roku 2009 bol tento počet približne 74 miliónov a v roku 2010 mal hodnotu vyše 580 miliárd. Takýto neuveriteľný nárast je spôsobený nielen rozšírením internetu ale aj nárastom predaja tzv. múdrych telefónov – „smart – phones“ a tabletov. Štatistika však nie je konečná. Z výročnej správy za rok 2013 firmou Kaspersky Security vyplýva, že ich produkt zneškodnil alebo bol v konfrontácii s približne 5.2 biliónom kyber útokov[62]. To je viac ako 10 násobný nárast oproti roku 2010 a viac ako 80 násobný nárast oproti roku 2007.

[60] INTERNET WORLD STATS. *Internet growth statistics* [online]. 2014 [cit. 2014-05-05]. Dostupné z: http://www.internetworldstats.com/emarketing.htm
[61] SECURELIST. *Kaspersky Security Bulletin* [online]. 2010 [cit. 2014-05-05]. Dostupné z: http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010
[62] SECURELIST. *Kaspersky Security Bulletin* [online]. 2013 [cit. 2014-05-05]. Dostupné z: https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

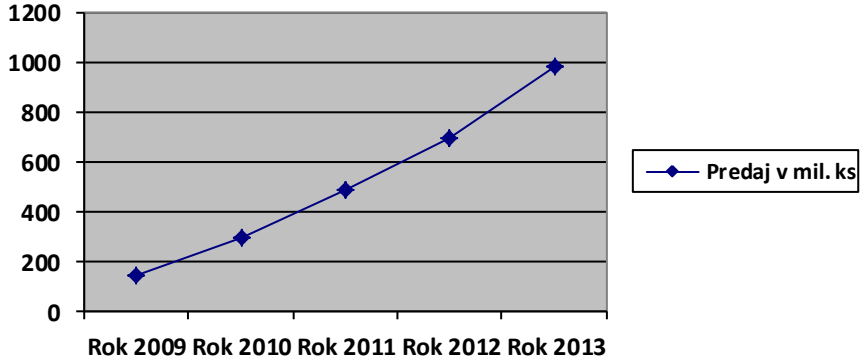
Graf 5 - Počet útokov na používateľov Kaspersky Security



Zdroj: spracované na základe dát z *Kaspersky Security Bulletin*

Tento rapídny skok majú za následok aj spomínané smart-phony. Ich predaj bol v roku 2009 niekde na úrovni 146 milónov[63]. V roku 2010 sa tento predaj zvýšil na približne 298 milónov[64]. V roku 2011 sa takmer zdvojnásobil na počet 486 miliónov, rok 2012 vykazoval hodnotu približne 698 miliónov a rok 2013 sa ukončil na približnej hodnote 990 miliónov[65]. Tento stúpajúci trend je nezastaviteľný.

Graf 6 - Predaj inteligentných telefónov od roku 2009



Zdroj: spracované autorom na základe dát z *Communities dominate*

[63] COMMUNITIES DOMINATE BRANDS. *Final 2009 mobile phone market numbers* [online]. 2010 [cit. 2014-05-05]. Dostupné z: http://communities-dominate.blogs.com/brands/2010/03/final-2009-mobile-phone-market-numbers-as-all-have-reported-we-have-big-news.html

[64] COMMUNITIES DOMINATE BRANDS. *Smartphone Bloodbath 2010* [online]. 2011 [cit. 2014-05-05]. Dostupné z: http://communities-dominate.blogs.com/brands/2011/02/smartphone-bloodbath-2010-now-final-numbers-q4-and-full-year-2010-and-each-rival-awarded-their-final.html

[65] COMMUNITIES DOMINATE BRANDS. *2013 Full year smartphone sales statistics* [online]. 2014 [cit. 2014-05-05]. Dostupné z: http://communities-dominate.blogs.com/brands/2014/02/final-2013-smartphone-market-share-numbers-full-year-and-quarterly-q4-data-by-top-10-brands-plus-os-.html

Čoraz viac ľudí podľahlo čaru múdrych telefónov a ich predaj je závratný. Je vidieť priamy súvis medzi predajom inteligentných telefónov a stúpajúcou tendenciou počítačových útokov. Taktiež je možné vidieť súvis medzi stúpajúcou intenzitou používateľov internetu a útokmi na nich. Pri tomto fenoméne platí, že čím väčšia je množina používateľov, tým viac rastie chuť a snaha o napadnutie ich.

5.4 Novinky v oblasti chránenia občanov Európskej únie pred kyberútokmi.

Aj vzhľadom na spomenuté fakty sa EÚ presvedčila a preto 11. januára 2013 bolo založené Európske centrum boja proti počítačovej kriminalite s názvom EC^3, ktoré má za úlohu posilniť výkon práva ako odpoveď na kyberzločiny v EÚ a týmto spôsobom pomôcť ochraňovať Európskych občanov a obchod v rámci EÚ[66].

EC^3 má za úlohu zaostriť na nasledovné tri oblasti:

1) Kyberzločiny spáchané organizovanými kriminálnymi skupinami, hlavne tými, ktoré generujú veľký profit zo zločinu ako napríklad on-line podvody a sprenevery.
2) Kyberzločiny ktoré spôsobujú vážne škody a ujmy ich obetiam ako napríklad on-line detské sexuálne zneužívanie.
3) Kyberzločiny, ale aj kyberútoky, ovplyvňujúce hlavné infraštruktúry a informačné systémy v únii.

EC^3 má za úlohu štyri hlavné funkcie a to :

1) Slúžiť ako informačná základňa boja proti počítačovej kriminalite.
2) Zhromažďovať európske odborné znalosti o počítačovej kriminalite v záujme podpory členských štátov pri budovaní kapacít.
3) Poskytovať členským štátom podporu pri vyšetrovaní počítačovej kriminality.
4) Stať sa spoločným hlasom európskych vyšetrovateľov z orgánov presadzovania práva a justície zameraných na počítačovú kriminalitu.

Podľa nedávneho prieskumu Eurobarometra bol napadnutý e-mailový klient alebo profil na sociálnych sieťach približne každému 8. občanovi v EÚ ktorý používa internet. Taktiež približne každý 14. občan sa stal obeťou podvodu v súvislosti s platobnou kartou či internetbankingom[67].

[66] EUROPOL. *European Cybercrime Centre (EC3): First year report* [online]. 2014 [cit. 2014-05-05]. Dostupné z: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report
[67] EUROPA.EU. *Prvý rok Európskeho centra boja proti počítačovej kriminalite* [online]. 2014 [cit. 2014-05-05]. Dostupné z: http://europa.eu/rapid/press-release_IP-14-129_sk.htm

V roku 2013, teda v prvom roku fungovania organizácie sa podarilo EC^3 pomáhať pri koordinácii 19 veľkých operácii boja proti organizovanej počítačovej kriminalite a aj z ich podporou sa podarilo rozložiť skupinu, ktorá rozposielala škodlivý mallware, ktorý zablokoval funkčnosť prehliadača, obvinil užívateľa z nelegálneho navštevovania web stránok a žiadal o zaplatenie 100 EUR pokuty. Nainfikovaných bolo niekoľko desiatok tisíc počítačov po celom svete.

6 Záver

Problém počítačovej kriminality je v momentálnej dobe veľmi diskutovaným a skloňovaným pojmom. Zaslúži si istú dávku pozornosti, ako zo strany orgánov činných v trestnom konaní, tak zo strany odbornej a laickej verejnosti. V mojej bakalárskej práci som sa snažil stručne popísať historický a momentálny vývoj počítačovej kriminality a jej napredovanie. Snažil som sa snažil poukázať na problematiku sociálneho hackingu, jeho definíciu a upozorniť na hroziace nebezpečenstvo. Taktiež sa v práci definuje a právne vymedzuje pojem hacker a hacking. Práca sa zaoberá aj dopadmi počítačovej kriminality na ekonomiku.

Počítačová kriminalita môže postihnúť značnú šírku osobného a spoločenského života. Výpočtová technika je nasadená vo všetkých správach štátu, či už v armáde, polícii, v priemysle, zdravotníctve a i. Ako už v mojej práci bolo mnoho krát spomenuté, počítačová kriminalita svojou podstatou presahuje územné hranice jednotlivých štátov a kontinentov, čiže sa stáva nadnárodným zločinom. Preto jednotlivé právne ustanovenia a zákony štátov na problematiku nestačia. Musíme k nej teda pristupovať inak.

V úvodnej kapitole som sa venoval teoretickému výkladu všeobecného pojmu *počítačová kriminalita.* Od historických počiatkov až po súčasnosť, jej definícia a snažil som sa zamerať na najznámejšie prípady jednotlivých období. Za veľmi potrebné som považoval zoznámiť čitateľov s historickým vývojom tohto expandujúceho nového druhu kriminality spoločne s jeho vývojom až do dnes. V druhej kapitole som sa zameral na formy a druhy počítačovej kriminality, ako aj na osoby, ktoré tieto delikty páchajú. Taktiež som v kapitole rozobral rôzne možnosti páchania zločinov.

V tretej, hlavnej a najrozsiahlejšej kapitole som sa zaoberal problematikou sociálneho hackingu. Definoval som pojem a snažil som sa ho na príkladoch ukázať čitateľom. Pri poukazovaní na otvorenosť a dostupnosť informácii zo sociálnych sietí sa podarilo čiastočne potvrdiť hypotézu, že sociálne siete sa stali zdrojom na obchodovanie a zneužívanie osobných dát. V kapitole sa spomínajú aj monitorovacie možnosti a schopnosti jednotlivých štátnych a súkromných zložiek po celom svete. Čo raz viac zasahujú do súkromia používateľov internetu. Môžeme teda hovoriť o neustálom sledovaní z viacerých strán. V tomto prípade sa podarilo čiastočne potvrdiť ďalšiu hypotézu a teda monitorovanie ľudí štátnymi a súkromnými zložkami neslúži iba na bezpečnosť a ochranu.

Zameral som sa aj na problematiku *cloud computeringu* a jeho technických výhod a nevýhod. Na prípadné možnosti odškodnenia pri rôznych nečakaných udalostiach. Posledná kapitola bola venovaná ekonomickým a právnym dopadom hackingu. Táto téma je z ekonomického hľadiska však veľmi zložitá, až nemožná na získavanie relevantných a presných dát. Preto sa pohybujeme v sfére odhadov. Ročne sú poškodení milióny používateľov po celom svete, no nie všetci sú si vedomí skutku, ktorý sa udial. Aj preto sú ekonomické dopady hackingu len ťažko vyčísliteľné. Na základe informácii, ktoré som získal, je možné čiastočne potvrdiť hypotézu, že svet internetu nie je taký anonymný a bezpečný, ako tomu bolo v minulých dekádach, kde útoky a sledovanie aktivity na internete nepatrilo medzi dennodenné praktiky. Z výsledkov vyplýva, že nárast je enormný aj vďaka rozšíreniu tzv. „smart-phone“ a tabletov. Internet sa tak dostáva čoraz bližšie k používateľovi a stáva sa jeho dennodennou a neoddeliteľnou súčasťou. Na základe nepresnosti a neúplnosti dát a informácii nebolo možné potvrdiť hypotézu, že počítačová kriminalita a sociálny hacking sú najbežnejším javom za poslednú dekádu, ktorý napĺňa skutkovú podstatu trestného činu. Neexistujú štatistky, ktoré by presne dokázali odlíšiť „bežnú“ kriminalitu od tej počítačovej a zároveň neexistuje možnosť presne vyjadriť množstvo počítačovej kriminality na svete.

Záverom možno skonštatovať, že nech sa budú vyvíjať informačné technológie akýmkoľvek smerom, boj s počítačovou kriminalitou je márny, pokiaľ sa nezjednotia právne zložky štátov v jednotlivých krajinách. Internet nemá hranice a je obmedzovaný iba v niektorých krajinách. Treba však brať ohľad aj na používateľov, ktorých úmysly sú čisté a mieru sledovania a obmedzovania prispôsobiť tak, aby sa predišlo špehovaniu všetkých používateľov. Potom by slobodný a neobmedzený internet stratil svoj zmysel.

Zoznam použitej literatúry

BRENNER, Susan W.. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. UPNE, 2012. ISBN 1555537995, s. 263

JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, 2007. ISBN 80-2471-561-2, s. 284

MATĚJKA, Michal. *Počítačová kriminalita*. 2002. vyd. Praha: Comupter Press, 2002. ISBN 80-7226-419-2, s.106

SMEJKAL, Vladimír a i. *Počítačové právo*. 1 vyd. Praha: C. H. Beck/SEVT 1995. ISBN 80-7179-009-5, s. 264

ŠÁMAL, Pavel a kol. *Trestní zákoník I: Komentář*. 1. vyd. Praha: C. H. Beck, 2009. ISBN 9788074001093, s. 3285

Zákon č. 40 z dňa 8. januára 2009 Trestný zákonník, In: *Sbírka zákonů České republiky*. 2009 Dostupný z : *www.mvcr.cz/soubor/sb011-09-pdf.aspx* . ISSN 1211-1244

Zákon č. 127 z dňa 22. februára 2005 o elektronických komunikáciách a o zmene niektorých súvisiacich zákonov(zákon o elektronických komunikáiach) In: *Sbírka zákonů České republiky.*

Zákon č. 480 z dňa 29. júla 2004 o niektorých službách informačnej spoločnosti In: *Sbírka zákonů České republiky.*

Dohoda Rady Európy o počítačovej kriminalite (Convention on Cybercrime, ETS No. 185), Budapešť, 23.11.2001, dostupná z : http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm,

Štrasburský protokol (ETS No. 189) k dohode Rady Európy o počítačovej kriminalite, dostupné z : http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm,

Manuál OSN pre prevenciu a kontrolu počítačového zločinu, dostupné z: http://www.uncjin.org/Documents/EighthCongress.html

KRAPP, Peter. Terror and Play, or What Was Hacktivism?. *MIT Press Journals*. 2005, roč. 5, č. 19, s. DOI: 1526-3819

CHIP: Pirátvstí v číslech. Praha: CHIP Holding G.m.b.H, 2012, roč. 22, č. 5. ISSN 1210-0684.

CHIP: Tajné síly na INTERNETU. Praha: CHIP Holding G.m.b.H, 2013, roč. 23, č. 2. ISSN 1210-0684

CHIP:Proč jsem PODEZŘELÝ. Praha: CHIP Holding G.m.b.H, 2012, roč. 22, č. 10, ISSN 1210-0684

Elektronické zdroje

http://arstechnica.com/

http://byznysplac.cz

http://communities-dominate.blogs.com

http://conventions.coe.int

https://www.datenschutz-hamburg.de

http://edi.fmph.uniba.sk

http://eeur.trendmicro.eu/

http://epp.eurostat.ec.europa.eu/

http://europa.eu

https://www.europol.europa.eu

http://www.ftc.gov

http://ftp.arl.mil/

http://www.hoax.cz

http://www.indect-project.eu

http://www.internetworldstats.com

http://www.itu.int/

http://lyceum-oajh.wz.cz

http://www.mckinsey.com

http://www.mitpressjournals.org

http://www.mojandroid.sk

http://now-static.norton.com

http://www.oxforddictionaries.com

http://pc.zoznam.sk

http://royal.pingdom.com/

http://www.securelist.com

http://www.securityweek.com

https://snowplow.org/tom

http://www.slsp.sk

http://www.statisticbrain.com

http://www.svetit.sk/

http://www.switched.com

http://www.symantec.com

http://tech.sme.sk

http://transition.fcc.gov/

Zoznam skratiek

CIA	Central Intelligent Agency- Centrálna spravodajská služba
EUR	Euro
EÚ	Európska únia
mld.	miliardy
ods.	odstavec
písm.	písmeno
S.z	sbírka zákonů
USD	Americký dolár
TrZ	Trestný zákonník

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byl(a) seznámen(a) s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 7.5.2014

.....

jméno a příjmení studenta

Zoznam Príloh